

Trellix

24-26 OCTOBER 2023

EMEA Security Summit Rome, Italy



Welcome

EMEA Security Summit • Rome, Italy • October 24 - 26



TODAY'S AGENDA

EMEA Security Summit • Rome, Italy • October 24 - 26

REGISTRATION

8:00am – 9:00am Registration Open

KEYNOTE SESSION

9:30am – 9:40am **Welcome & Introduction**
Fabien Rech, Senior Vice President EMEA

9:40am – 10:00am **Trellix CEO Keynote**
Bryan Palma, Chief Executive Officer

10:00am – 10:30am **Mind of a Trellix CISO**
Harold Rivas, Chief Information Security Officer

10:30am – 11:00am **Unveiling the Shadows**
John Fokker, Head of Threat Intelligence, Trellix ARC
Mo Cashman, Field CTO EMEA

11:00am – 11:15am **Perspectives from a Trellix Security Alliance Partner**
Harrison Holstein, Global Architect, AWS

11:15am – 11:40am **Panel Discussion**
Moderated by Vibin Shaju, VP Solution Engineering, EMEA

11:40am – 11:50am **Closing**
Fabien Rech, Senior Vice President EMEA

NETWORKING LUNCH

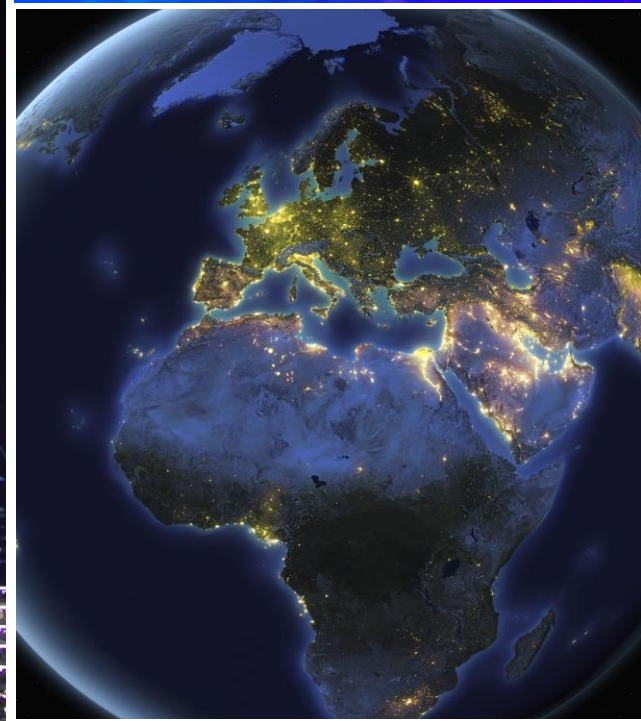
12:00pm – 1:30pm **Networking Lunch**

01:30pm - 5:15pm **Breakout Sessions**

5:30pm – 7:30pm **Networking Reception**



Trellix



WHERE is Trellix Coming From?

Trel·lis

['trelis]

NOUN

**BIOLOGY, WELLNESS,
SUSTAINABILITY**

A framework used to support trees or plants.

Trel·lix



['trelix]

NOUN


CYBERSECURITY

A global ecosystem dedicated to **living security**, an open XDR architecture and experts inspired by cybersecurity's soulful work.








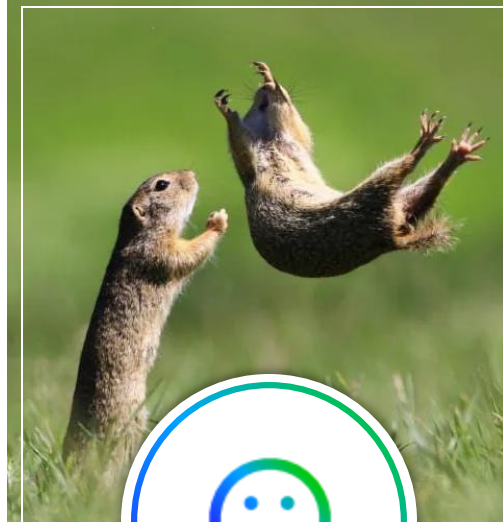
Open



Curious



Tenacious



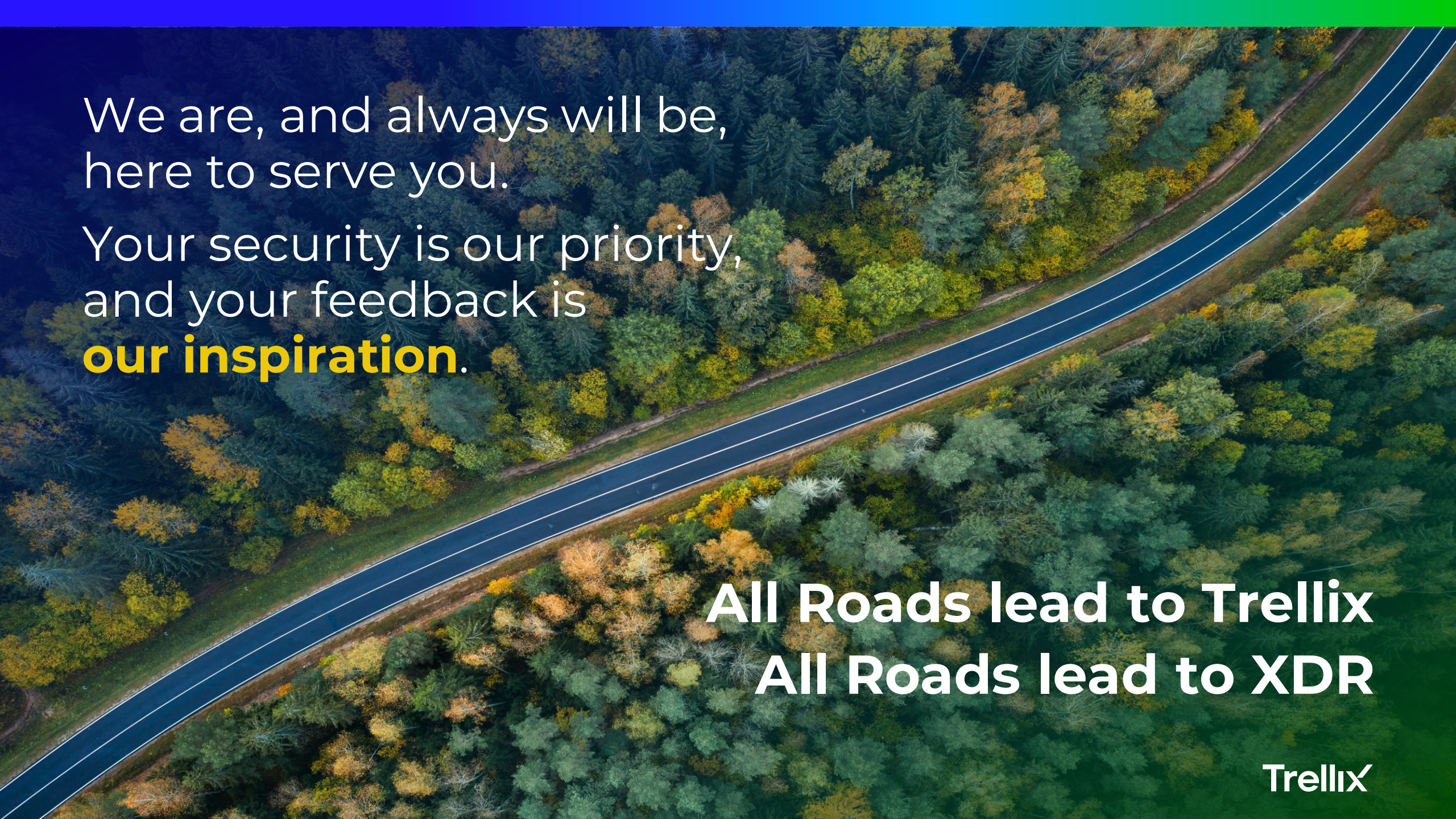
Fun



SOCIAL MEDIA

I have one ask: Please share photos, make some noise

Use hashtags [#TeamTrellix](#), [#Soulfulwork](#), [#TrellixXDR](#)

An aerial photograph of a two-lane asphalt road winding through a dense forest. The trees are in various stages of autumn, with some showing bright yellow and orange leaves, while others remain green. The road curves from the bottom left towards the top right of the frame.

We are, and always will be,
here to serve you.

Your security is our priority,
and your feedback is
our inspiration.

All Roads lead to Trellix
All Roads lead to XDR

Trellix

Trellix

Thank You!



Trellix

Mind of a Trellix CISO

Harold Rivas

October 24, 2023



25+ years of Information Security experience leading global programs for financial services and highly regulated organizations.

Served as CISO and senior technology leader for multiple international companies, including Fujitsu, loanDepot, Santander, Mr. Cooper, and Citigroup.

Lead the Trellix Information Security program leveraging the full suite of its capabilities (products, services, and partnerships).

Guide the Customer Zero program providing a customer's view and feedback loop into our product roadmap.

Harold Rivas

Chief Information Security Officer



Agenda



CISO Journey

- Historical Timeline

Threat Forecast

- New and Emerging Risks

SOC Battle Plan

- Evolving our approach to SecOps



CISO Journey

Historical Timeline

1995

Citi hires the first CISO; role was created to address growing risk of information security.

2002

- + Regulatory compliance era starts
- + CISOs become risk oriented
- + Vendor risk and the extended enterprise

2013

- + Cybersecurity is a major focus
- + Frameworks like NIST CSF adopted
- + Business Resilience DR/BCP

2023

- + Privacy laws impact CISOs
- + Data Governance
- + Cyber fraud



Threat Forecast

2024 and beyond

- Geopolitical conflicts
- Economic pressures
- Generative AI
- Evolution of OT risks
- Software Supply Chain
- Stronger regulations
- Accelerating Attacks
- Skills & staff shortages



“Before anything else,
preparation is the key
to success.”

Alexander Graham Bell





SOC Battle Plan

Evolving the approach to SecOps



Typical SOC Environment



Mix of Tools

Limited Visibility

Fragmented Control & Visibility
with Disparate Tools



Budget
& Staffing

Culture of Burnout

Navigating Alert Fatigue
& Limited Expertise



High Volume
of Log Events

Insufficient Coverage

Balancing Capacity
& Technical Skills



XDR = A better way forward

Threat focused, holistic view, guided response with fast containment actions

**People,
Processes,
Technology**



Develop your SOC
Analysts Faster

**Support
Consolidation
Initiatives**



An open platform to
support all your
security investments

**Enable Rapid
Containment
Actions**



Speed is essential in
minimizing the impact
of an incident

Focus on your threat actors

- ❑ Identify the top threat actors by industry, geography, association, etc.
- ❑ Combine and leverage threat intelligence on those actors.
- ❑ Institute controls based on real threat intelligence.
- ❑ Partner with executive leadership to meaningfully reduce risk.
- ❑ Share threat intelligence!

Automated Response

- ❑ Define a target (minutes/hours) for Mean Time to Contain (MTTC).
- ❑ Establish Board/Executive Level support for automated containment.
- ❑ Demand that every new platform your organization deploys integrates with your response platform to future-proof your investments.

Simplify your tech stack

- ❑ Platform fragmentation creates administrative overhead.
- ❑ Where possible consolidate platforms to reduce administrative burden.
- ❑ Seek an open ecosystem to ensure maximum SOC response speed.
- ❑ Support the growth and evolution of your SOC analysts

Trellix

Thank You!



Trellix

24-26 OCTOBER 2023

EMEA Security Summit
Rome, Italy





John Fokker

Head of Threat Intelligence at Trellix
Advanced Research Center



Mo Cashman

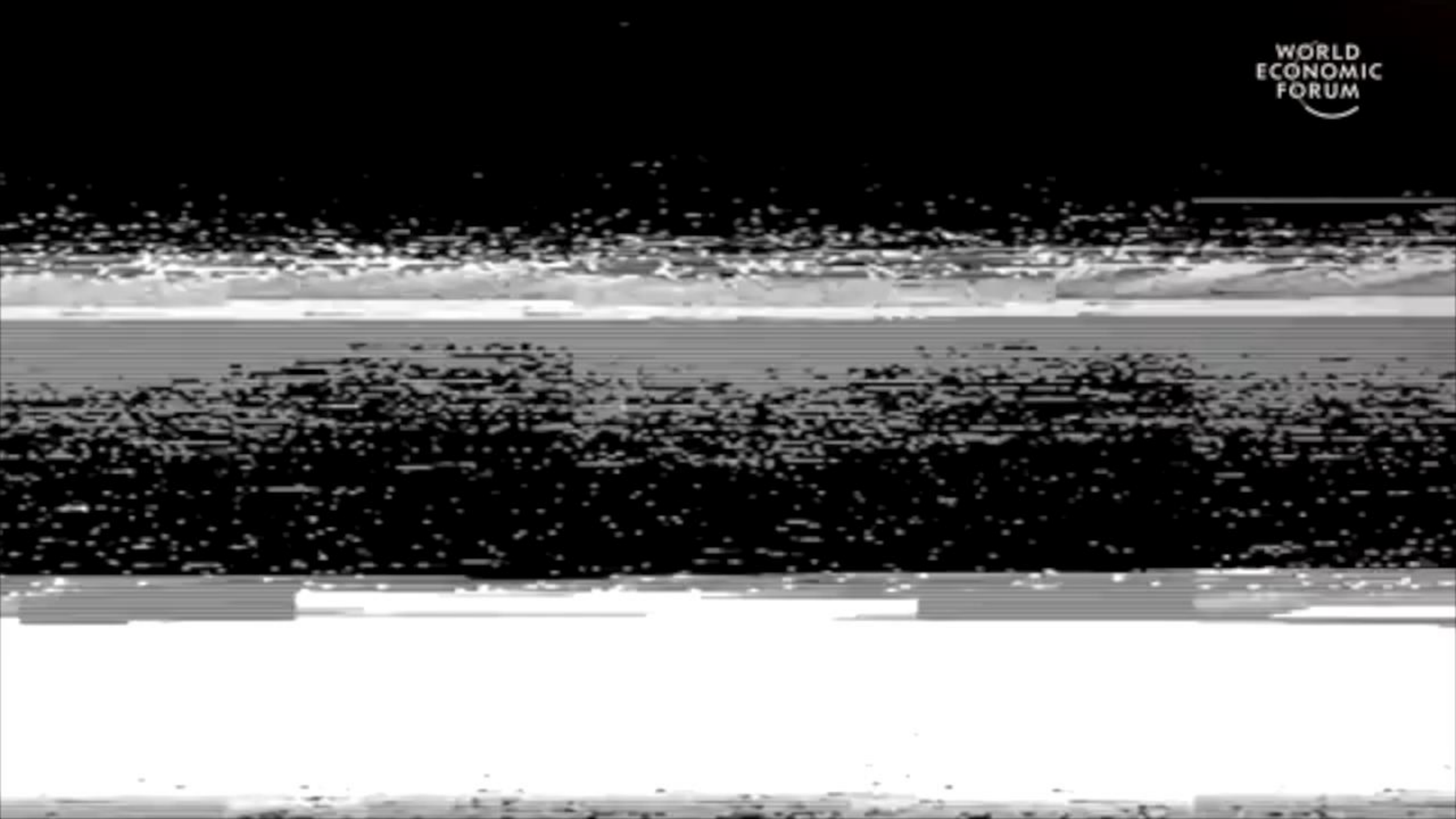
EMEA Field CTO, Trellix



Trellix

Unveiling the Shadows

Chaos to Clarity



WORLD ECONOMIC FORUM



TRELLIX



Polycrisis

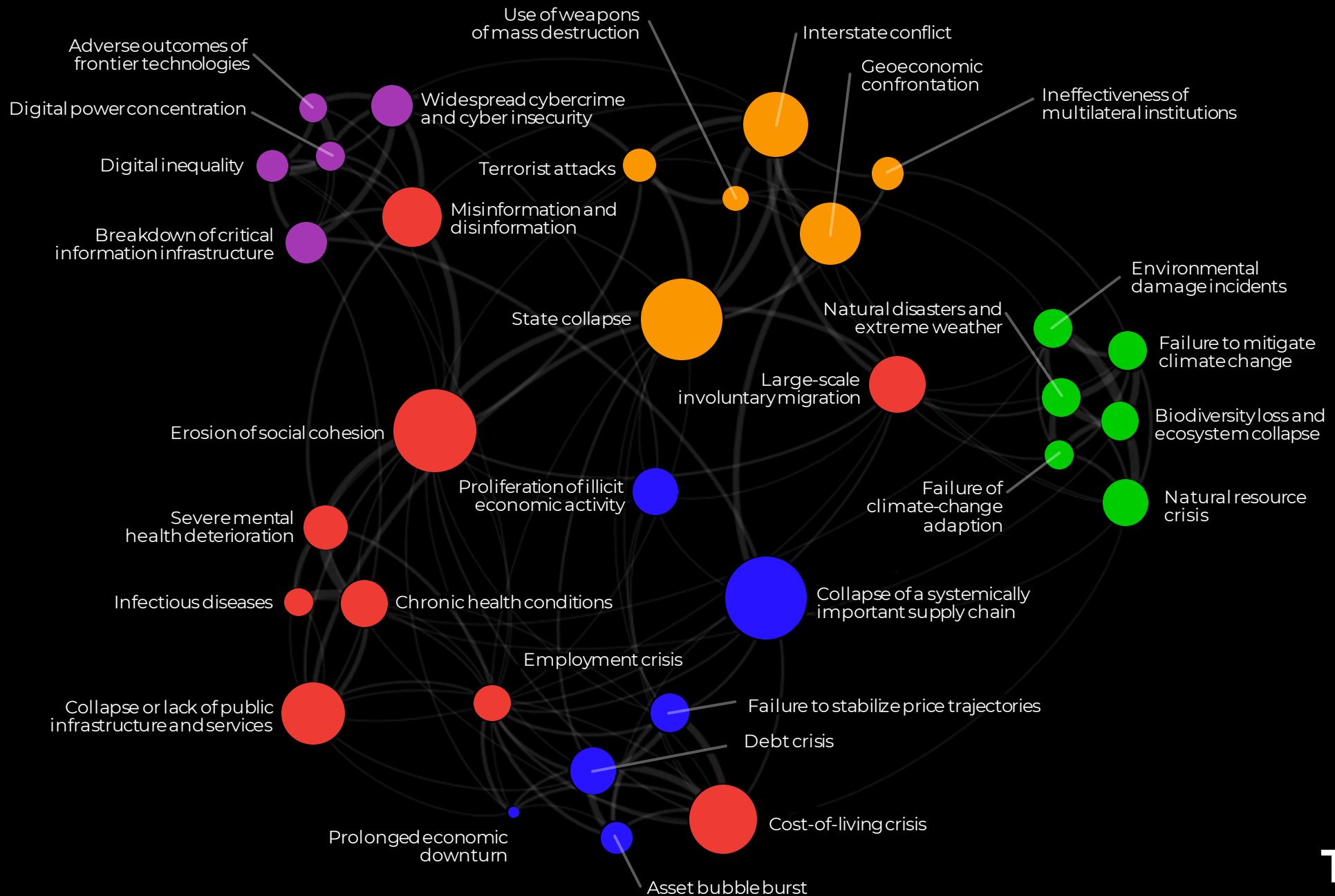


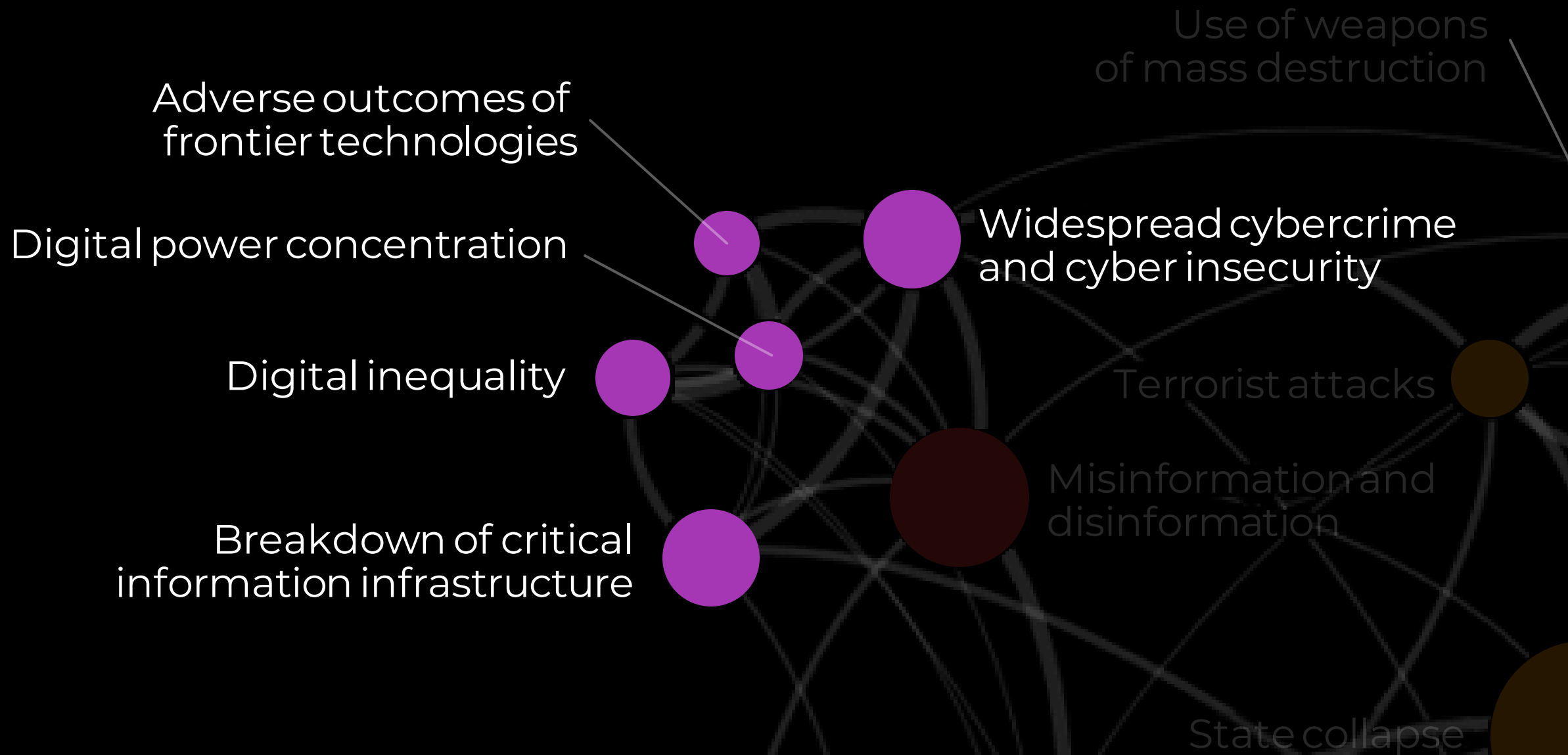
“ A cluster of related global risks with compounding effects, such that the overall impact exceeds the sum of each part ”.


The World Economic Forum's
[Global Risks Report 2023](#)

EMEA Polycrisis Reality Today: **2 wars across the region**









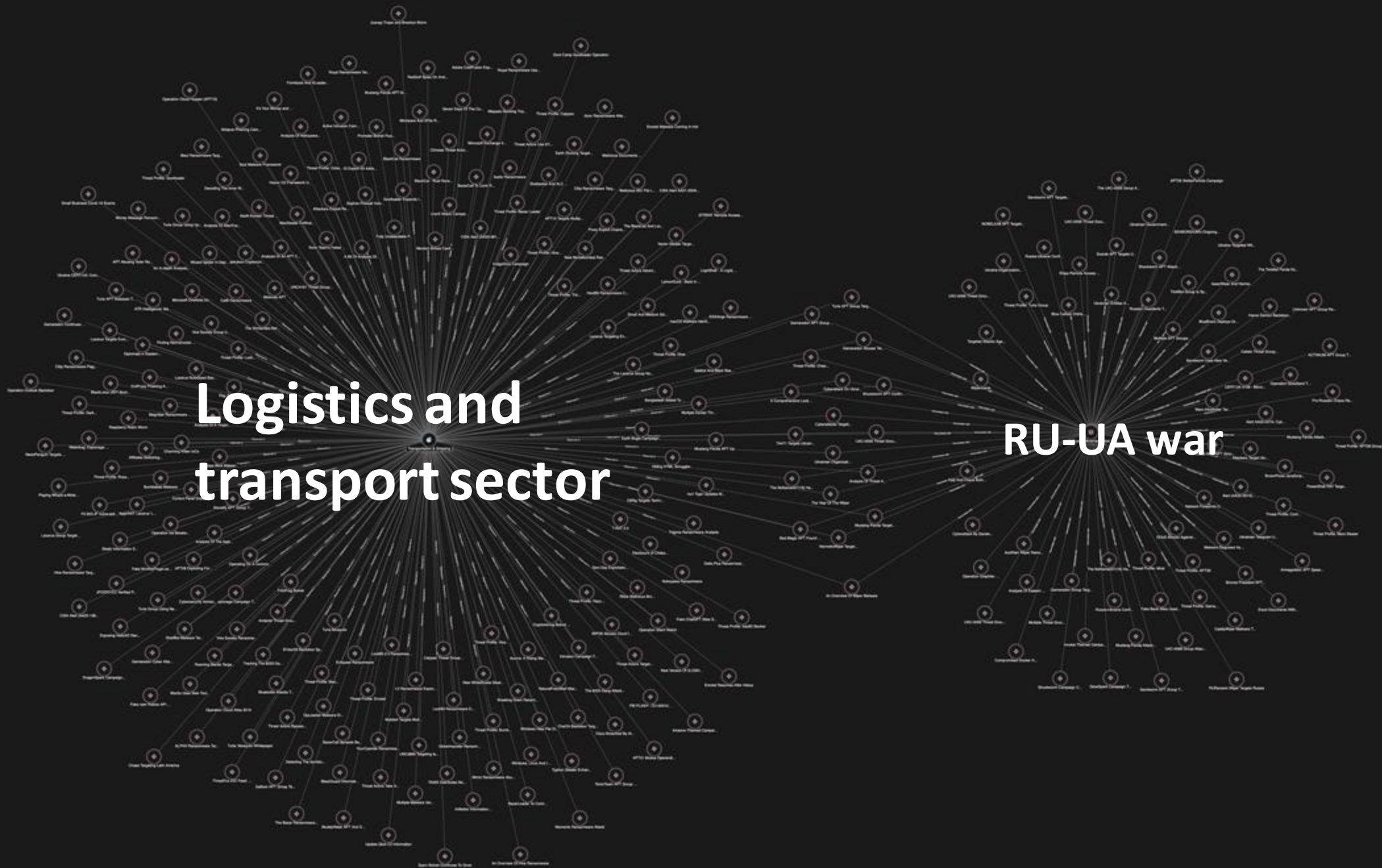
Cyber crime
thrives during
an era of
“Polycrisis”

**The World Economic Forum
defines a “polycrisis” as follows:**

*“A cluster of related global risks
with compounding effects, such
that the overall impact exceeds
the sum of each part”*

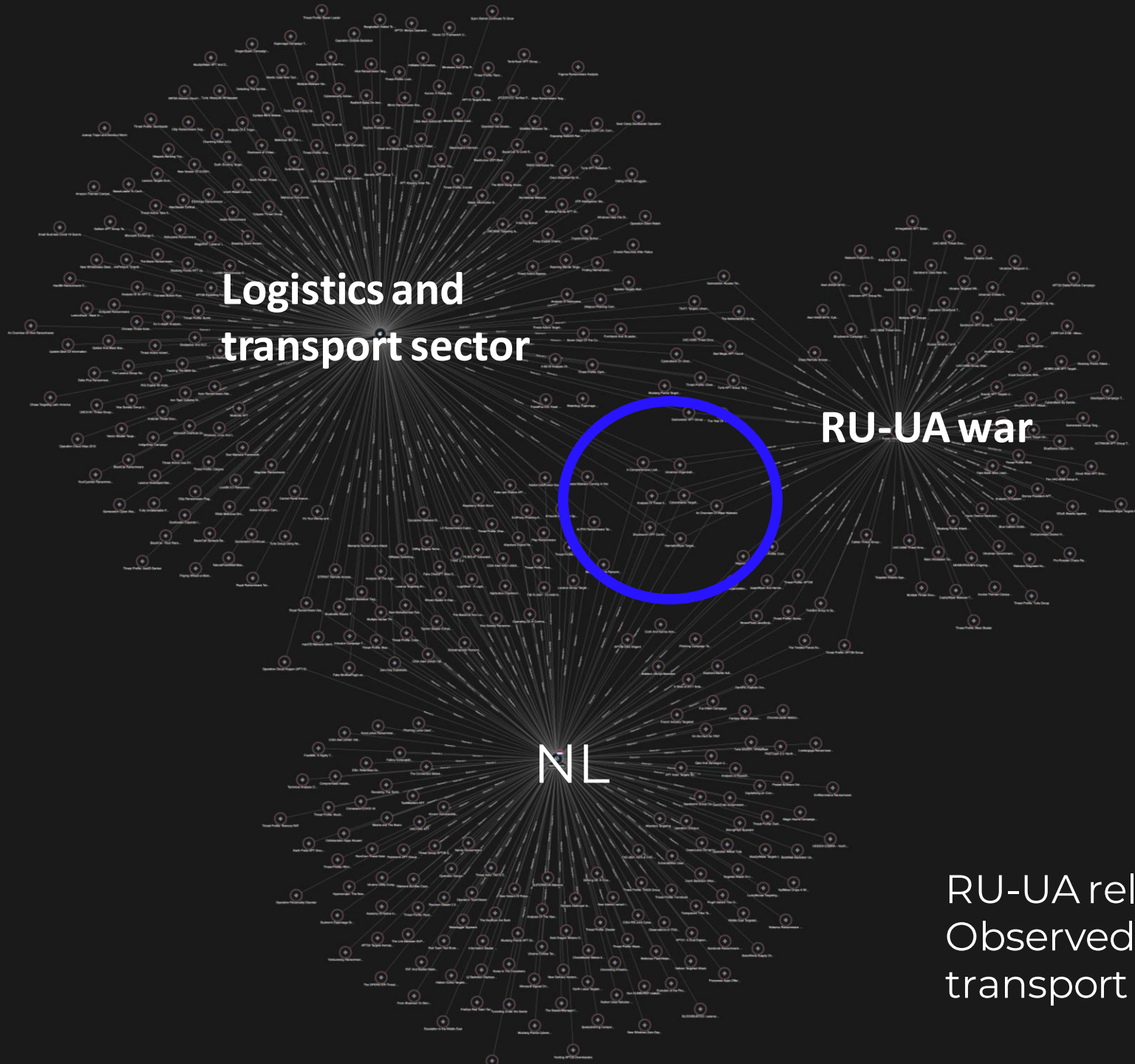
Reuters:

*“Often the transportation sector
finds itself at the heart of this
upheaval, both as victim and
protagonist.”*



**Logistics and
transport sector**

RU-UA war

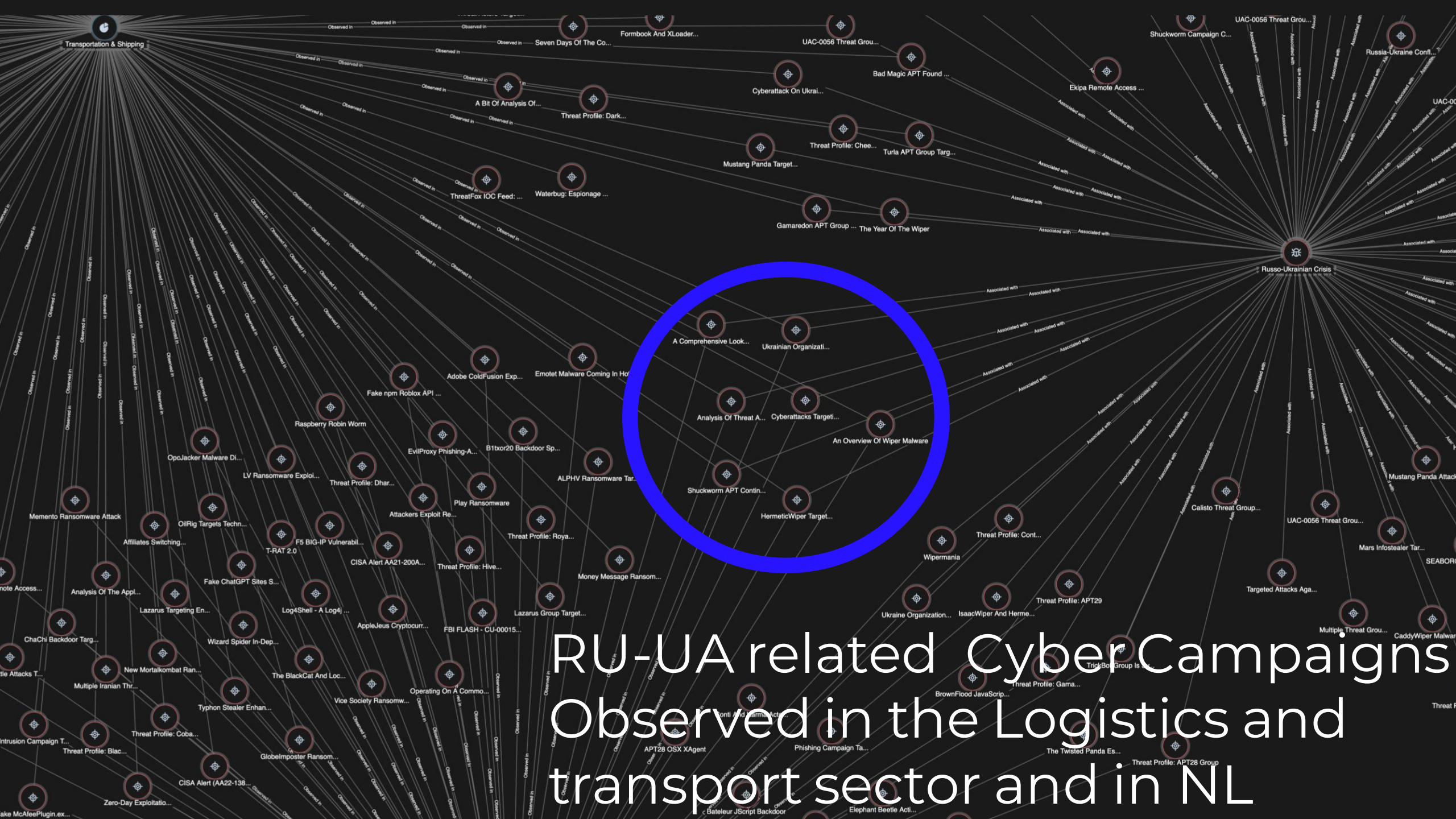


**Logistics and
transport sector**

RU-UA war

NL

RU-UA related Cyber Campaigns
Observed in the Logistics and
transport sector linked to NL



Transportation & Shipping

Russo-Ukrainian Crisis

RU-UA related Cyber Campaigns
Observed in the Logistics and
transport sector and in NL



**But are we
helpless against
a Polycrisis?**



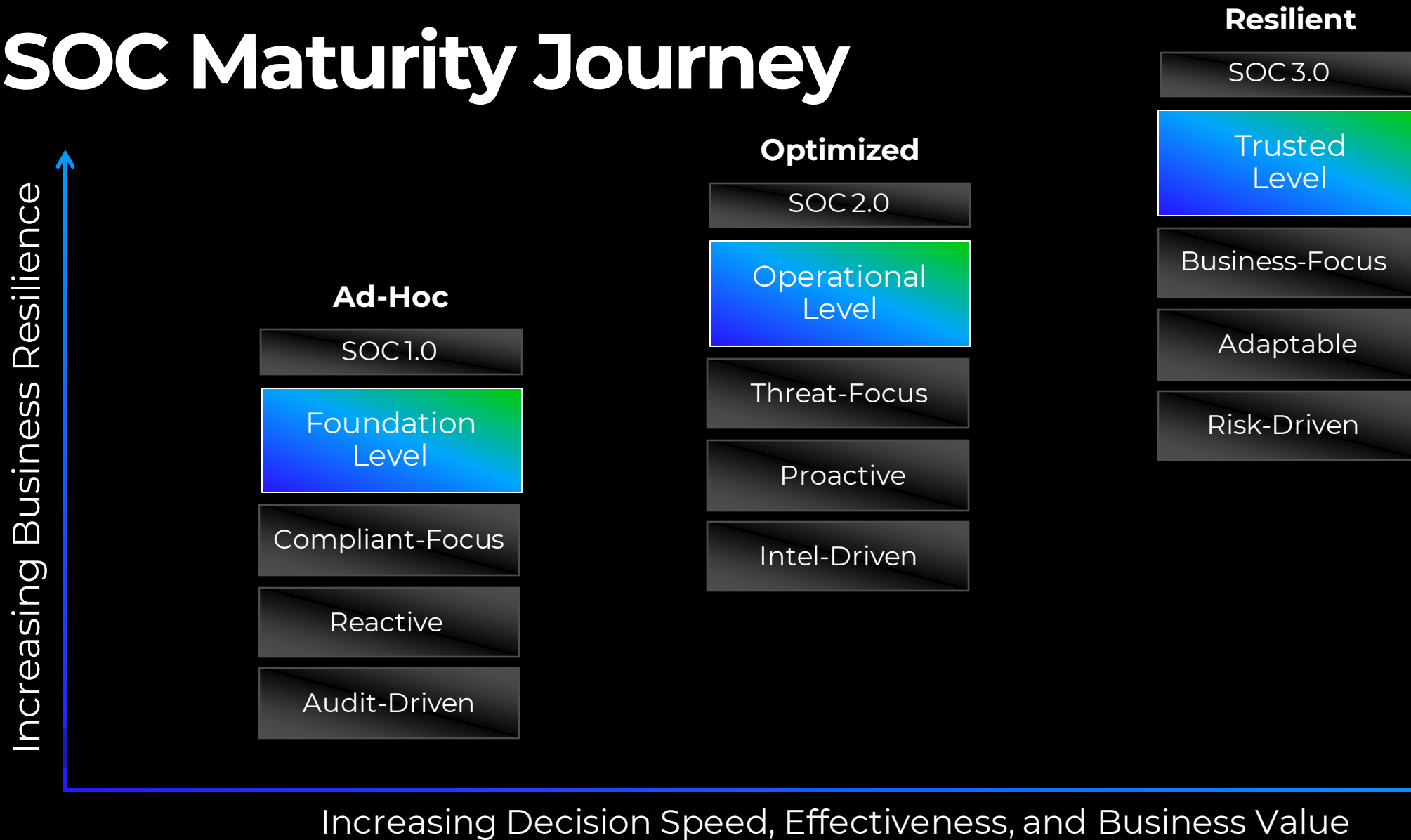
The Digital Operational Resilience Act (DORA)

Regulation (EU) 2022/2554

NIS 2 Directive

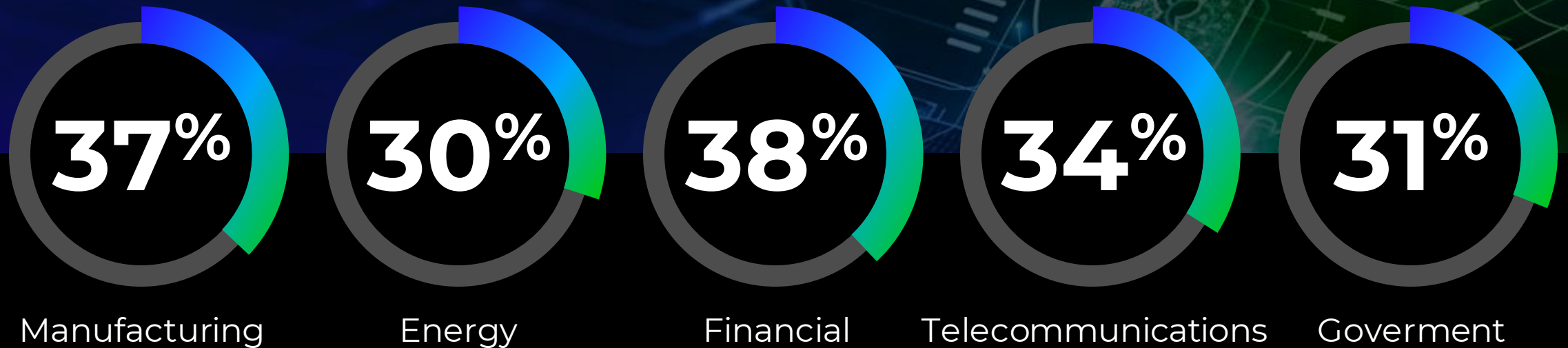


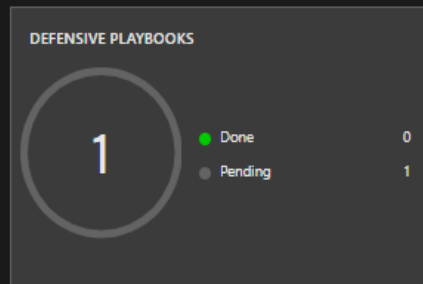
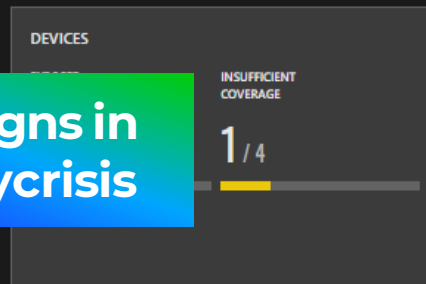
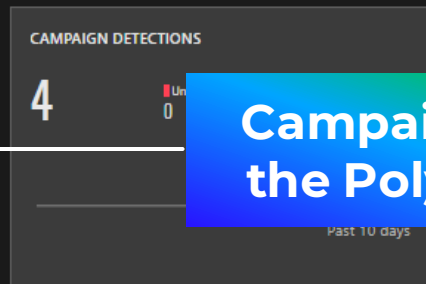
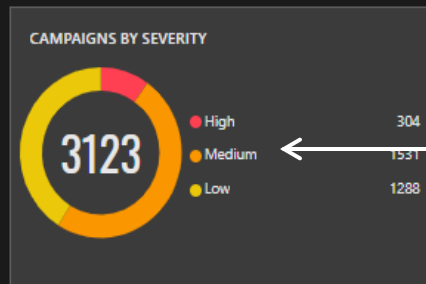
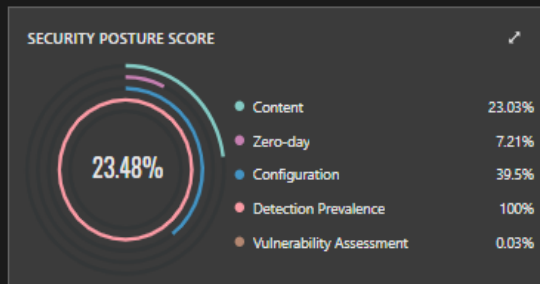
SOC Maturity Journey



Increasing Decision Speed, Effectiveness, and Business Value

State of Adaptability in Sec Ops





Campaigns in the Polycrisis

Campaigns Threats Profiles CVEs MITRE Explorer View more

Search Insights

Requiring Attention (1) All Campaigns (3123) Campaign Connections

Search Campaigns by Name

Sector: Government Country: United Kingdom Sort by: Last Detected

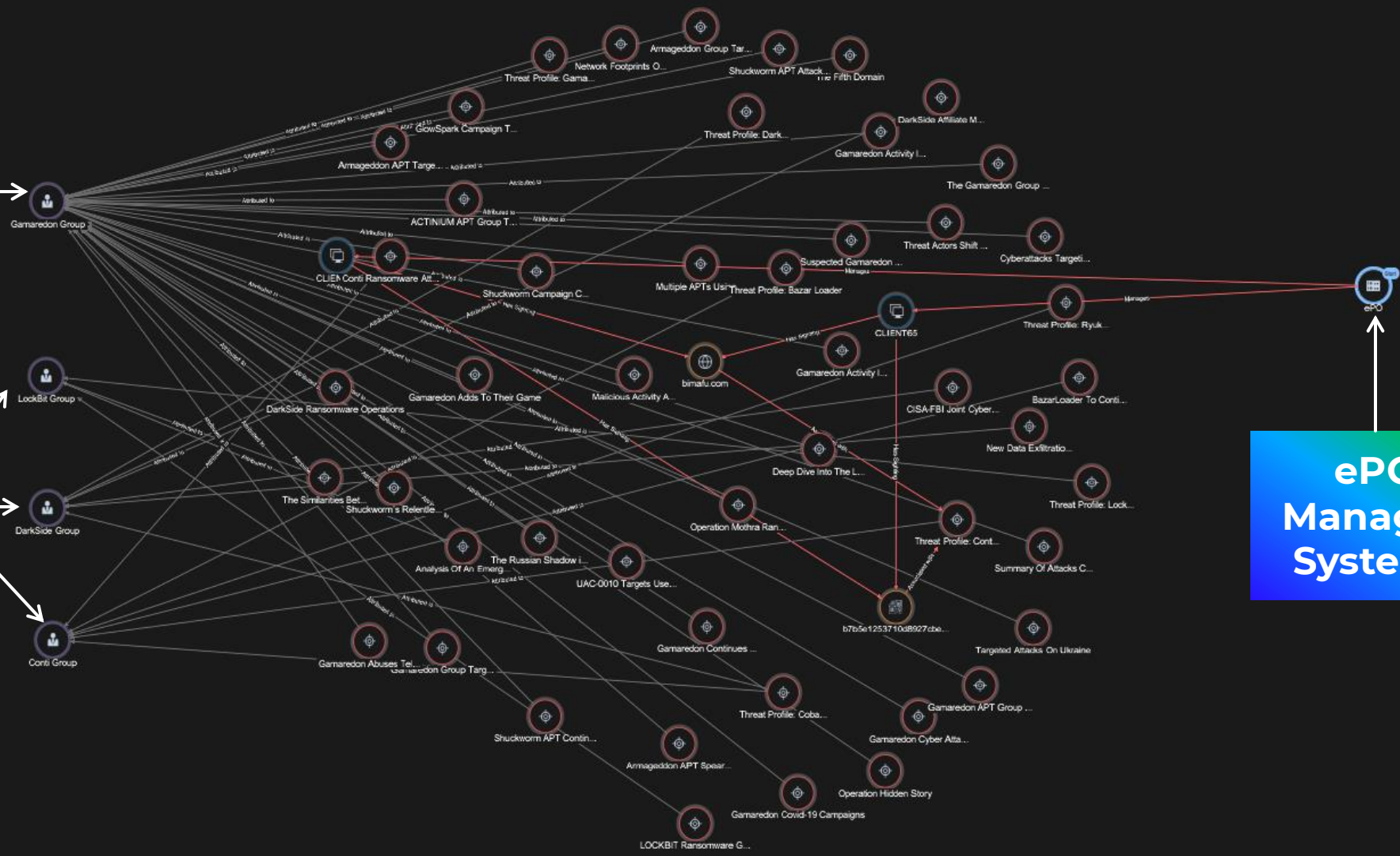
Campaign	Detection Comparison				Your Devices		Defensive Play...	Last Detected
	You	Government	GBR	Worldwide	Exposed Endpoints	Insufficient Coverage		
Threat Profile: Conti Ransomware	●	●	●	●	0	0	🔄 🛡️	5 hours ago
The Stealthy Email Stealer in the TA505 Arsenal	●	●	●	●	0	0	🔄 🛡️	Never
BlueNoroff APT Group Targets macOS With RustBucket Malware	●	●	●	●	0	0	🔄 🛡️	Never
B1txor20 Backdoor Spreading Via Log4j Vulnerability	●	●	●	●	0	0	🔄 🛡️	Never
PcShare backdoor attacks	●	●	●	●	0	0	🔄 🛡️	Never

Campaigns Affecting You

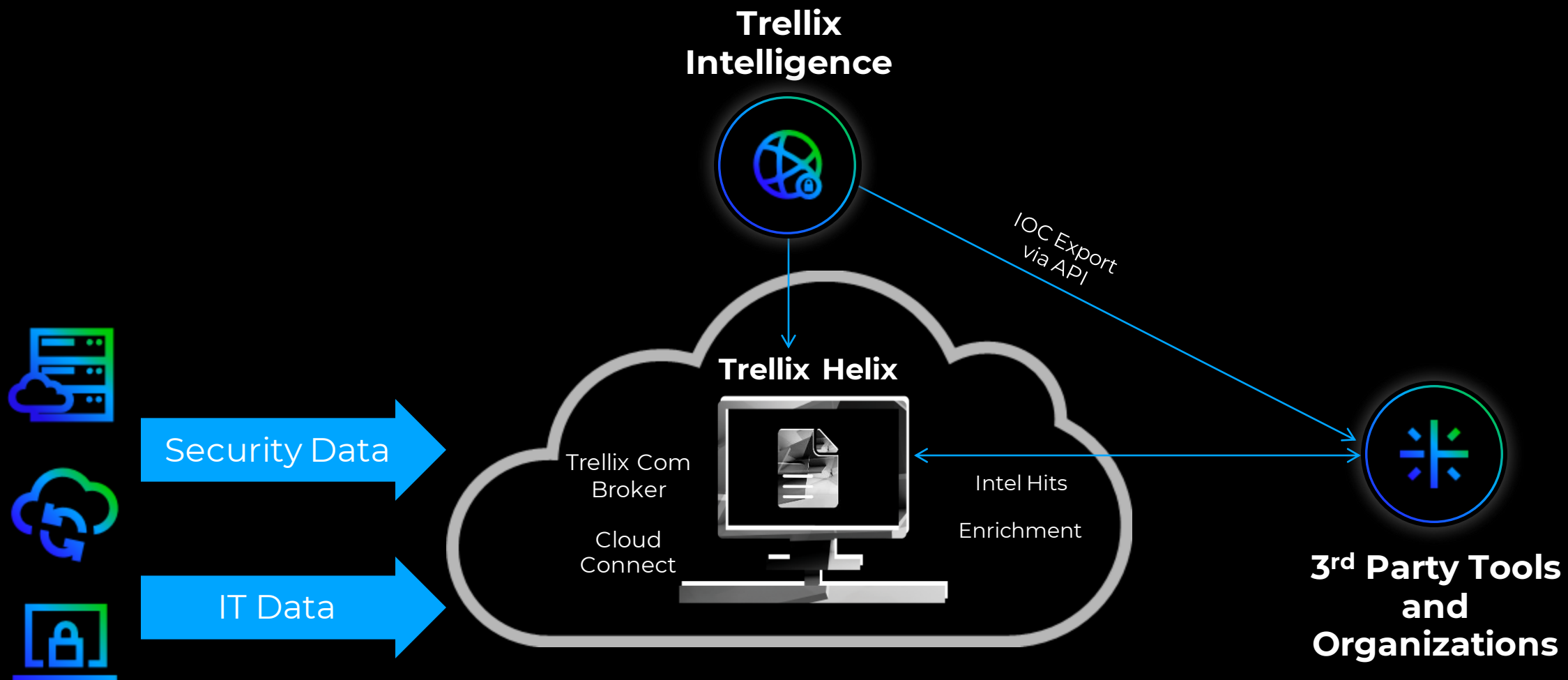
**APT Group
Gamaredon**

**Ransomware
Groups**

**ePO
Managed
Systems**



Sharing Threat Intel Across Borders



Trellix Intelligence From the Frontlines

Research Partner
Program



Research Partner Program In Action

Help those who
need it most...



SOGU Activity Discovery on Eastern European Participant



Overview

While conducting routine threat hunting for advanced threats, suspicious activity was identified with our Research Partner consistent with SOGU infection and persistence on a host belonging to Eastern European RPP participant.

Gamaredon /UNC530 TEMP. Armageddon attacks



Overview

During one of our Threat hunts, Trellix Threat Intelligence Group identified Gamaredon's Petrodo, which was targeting a Government organization. Gamaredon was leveraging specific PowerShell scripts and Wscripts for C2 communications.

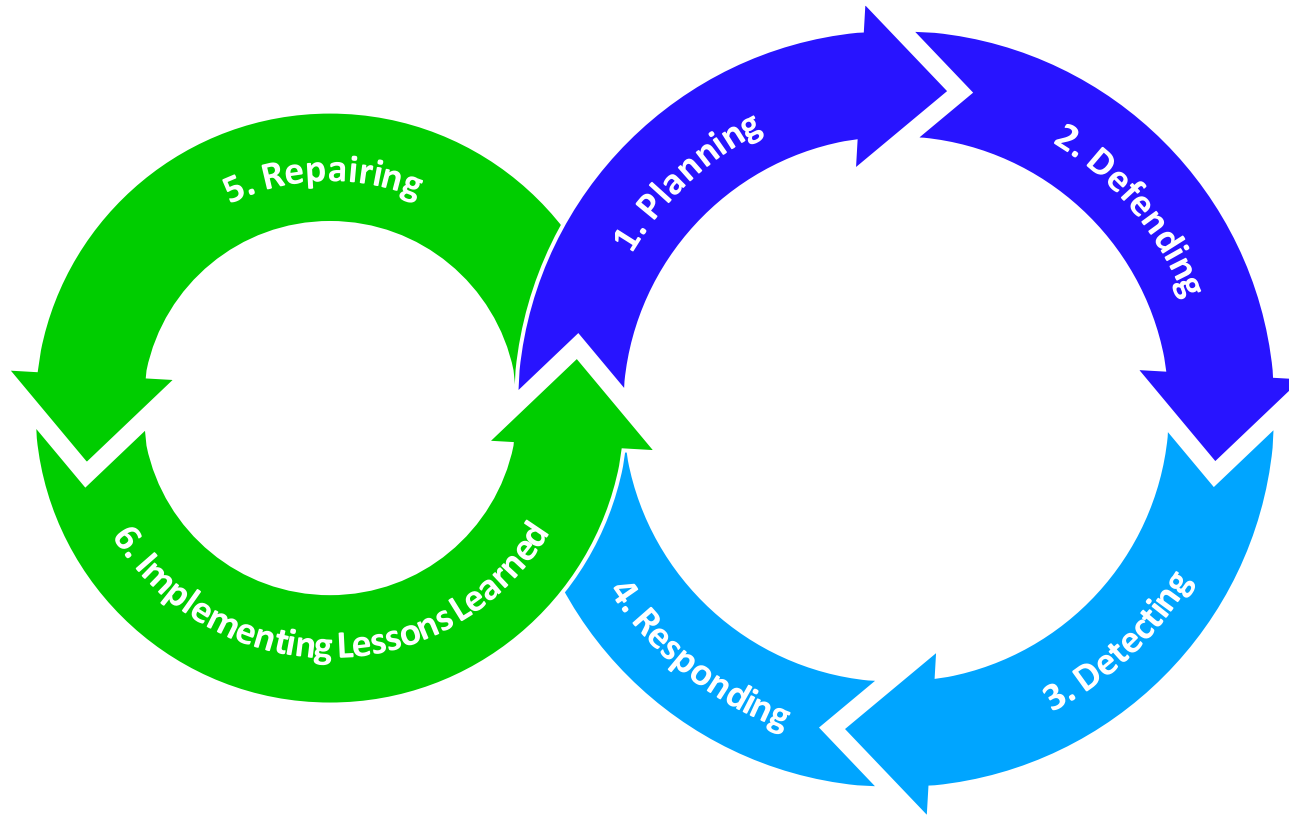
The C2 infrastructure was very dynamic. Threat actor created prevalence via schedule tasks and Logon Registry Keys.

**What can
you do?**



APT Defense is a constant process


Adaptable Security Lifecycle





The defense life cycle is a continuous process of **Preparation, Prevention, Detection and Mitigating Attacks**. When a ransomware attack is successful, the **Recovery** and **Root Cause Analysis** phases are triggered.


Identify APT Attacks Early



















ATT&CK Matrix for Enterprise

 Countermeasure Available

 Countermeasure Pending

 Countermeasure Completed

 Please note, the proposed countermeasure will not provide defense against all possible ways a tool can be used or the mentioned MITRE techniques as a whole. ✕

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Phishing 	Component Object Model	Boot or Logon Autostart Execution 	Boot or Logon Autostart Execution	Binary Padding	OS Credential Dumping	File and Directory Discovery	Internal Spearphishing	Audio Capture	Ingress Tool Transfer	Automated Exfiltration	Account Access Removal
Business Relationships	Botnet	Replication Through... 	Malicious File 	Office Application Startup 	Registry Run Keys / Startup Folder 	Compile After Delivery	/etc/passwd and /etc/shadow	Peripheral Device Discovery	Replication Through...	Automated Collection	Remote Access Software	Exfiltration Over C2 Channel	Application Exhaustion Flood
CDNs	Botnet	Spearphishing Attachment 	Malicious Link 	Office Template Macros 	Scheduled Task 	Deobfuscate/Decode Files or Information	ARP Cache Poisoning	Process Discovery	Taint Shared Content	Data from Local System	Web Protocols	Data Transfer Size Limits	Application or System Exploitation
Client Configurations	Cloud Accounts	Spearphishing Link 	Native API	Registry Run Keys / Startup Folder 	Abuse Elevation Control Mechanism	Disable or Modify Tools	AS-REP Roasting	System Checks	Application Access Token	Data from Network Share...	Web Service	Exfiltration Over Alternative...	Data Destruction
Code Repositories	Cloud Accounts	Cloud Accounts	PowerShell 	Scheduled Task 	Access Token Manipulation	File Deletion	Adversary-in-the-Middle	System Information Discovery 	Distributed Component...	Data from Removable...	Application Layer Protocol	Exfiltration Over Asymmetric...	Data Encrypted for Impact
Credentials	Code Signing Certificates	Compromise Hardware Supply...	Scheduled Task 	Accessibility Features	Accessibility Features	Impair Defenses	Bash History	System Owner/User Discovery	Exploitation of Remote Services	Screen Capture	Asymmetric Cryptography	Exfiltration Over Bluetooth	Data Manipulation
DNS	Code Signing Certificates	Compromise Software...	Visual Basic 	Account Manipulation	Active Setup	Masquerade Task or Service	Brute Force	User Activity Based Checks	Lateral Tool Transfer	ARP Cache Poisoning	Bidirectional Communication	Exfiltration Over Other Network...	Defacement
DNS/Passive DNS	Compromise Accounts	Compromise Software Supply...	Windows Command Shell 	Active Setup	AppCert DLLs	Masquerading	Cached Domain Credentials	Account Discovery	Pass the Hash	Adversary-in-the-Middle	Communication Through...	Exfiltration Over Physical Medium	Direct Network Flood

Requiring Attention (1) All Campaigns (3169) Campaign Connections

Connecting APT Intelligence to Detections

+ Search Campaigns by Name

Environment Country United Kingdom Sort by Last Detected

Campaign	Detection Comparison				Your Devices		Defens...	Last Detected
	You	Government	GBR	Worldwide	Exposed En...	Insufficient C...		
Armageddon APT Targets Ukraine With GammaLoad Malware	●	●	●	●	0	0	[Refresh] [Shield]	17 minutes ago
Gamaredon Continues To Target Ukraine But Shifts To Include NATO Allies	●	●	●	●	0	0	[Refresh] [Shield]	17 minutes ago
Threat Profile: Conti Ransomware	●	●	●	●	0	0	[Refresh] [Shield]	4 days ago

XDR = Visibility Across the Kill Chain

← THREAT LIST ID: 473564 Correlations Details

Assignee: Unassigned Status: Open Export Actions Fix Now Fix Now

About

Collection(+7) tactic(s) using Archive Collected Data(+12) technique(s) detected, but not blocked

CRITICAL 964

Collection(+7) tactic(s) using Archive Collected Data(+12) technique(s) detected, but not blocked on john.butter asset(s) by Endpoint Security.

Last Seen: 2023-10-21 18:07:05 UTC (a day ago)

Threat Prioritization

8/14 TACTICS

Open -- Unassigned

Overview Intel Events 67 Related Alerts 19 Related Assets 1 Response 0

Total Timeframe: 02d 55m 39s | Expand All Nodes Collapse All Nodes

Attack Visualization

Sensor Events

Endpoint Security → Did not block → Multiple Sources (7) → Which triggered → Multiple Alerts (19) → Involving → Multiple Assets (4) → From interacting with → Multiple Artifacts (34)

Multiple Alerts (19)

Node Contents

Risk Score	Name	Events	Alert ID
100	EDR credential search	5	5876945
100	Forensics IOC: rclone	4	5876951
100	EDR Trace credentials in Registry	1	5876937
80	AWS GUARDDUTY [unauthorizedaccess:s3/...	7	5877112
80	AWS GUARDDUTY [discovery:s3/maliciousu...	2	5876980
80	EDR Trace: RClone usage	1	5876941
75	DLP Alert: credentials access	2	5876949
70	EDR Trace: 7zip usage	1	5876943
70	IPS Medium Alert [login successful]	1	5876939
70	EDR Trace: WinSCP	1	5876944

Augment Built in Defences

Make Your Organization more Resilient with Trellix

Legacy Systems Protection

Trellix Application Control protects legacy Operating Systems

Email Security

Trellix Email Security protects against advance threats and business email compromise

Benchmark Assessments

Trellix Policy Auditor provides continuous monitoring to verify configuration against customer security benchmarks

Mobile Threat Protection

Trellix Mobile extends protection to Mobile Devices managed by Intune

Data Security

Trellix Data Security covers endpoint, network and databases

XDR

Trellix XDR provides Open XDR capability that detects threats using logs from Defender and O365 applications as well as Trellix security controls.

Forensics and OnPrem EDR

Trellix HX supplements Defender with additional visibility and investigative capability

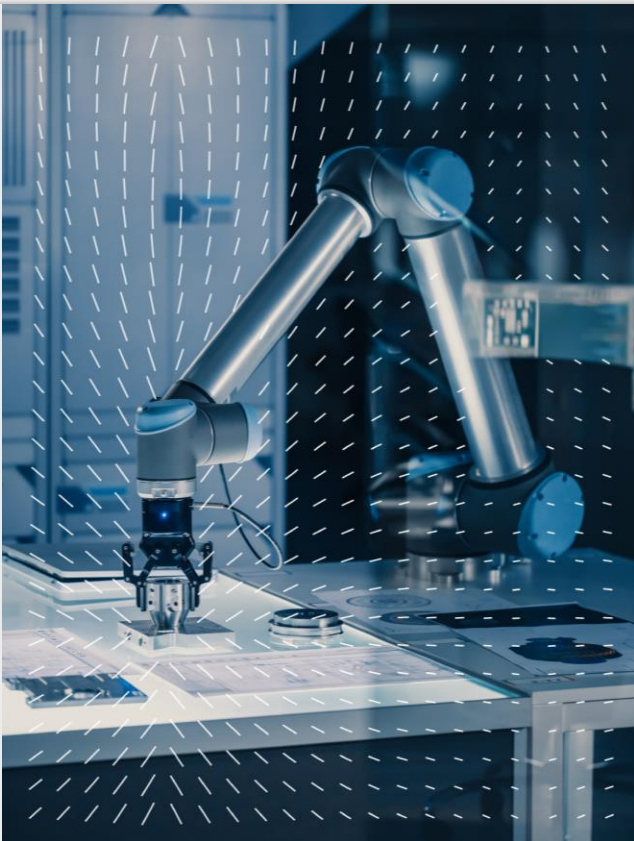
Threat Intelligence

Trellix Insights provides contextual threat indicators which can be imported into Defender or other SOC tools



Protect the critical systems

Lock Down Industrial Control, Medical and Financial Systems



ABB

Abbott

ALSTOM

EMERSON

HITACHI
MEDICAL SYSTEMS

Honeywell

NCR

PHILIPS

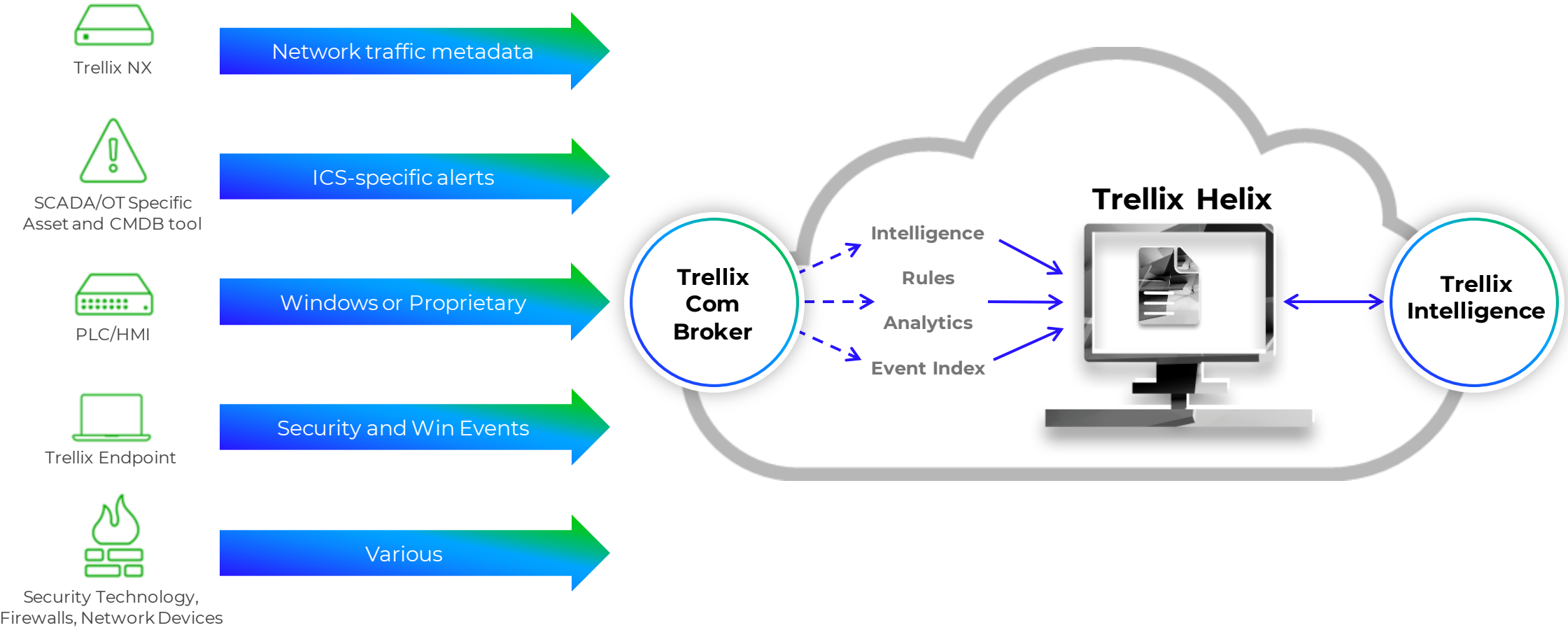
SIEMENS

Schneider
Electric

YOKOGAWA



OT Threat Detection and Response with XDR



ONLINE IDENTITY

A digital fingerprint scan graphic. The fingerprint is rendered in a glowing green color, set against a dark blue background with intricate circuit patterns. Vertical lines of light, some containing binary digits (0 and 1), appear to be scanning or interacting with the fingerprint. The overall aesthetic is futuristic and technological.

THIS WEBSITE HAS BEEN SEIZED



OPERATION COOKIE MONSTER



Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov



POLITI



AFP

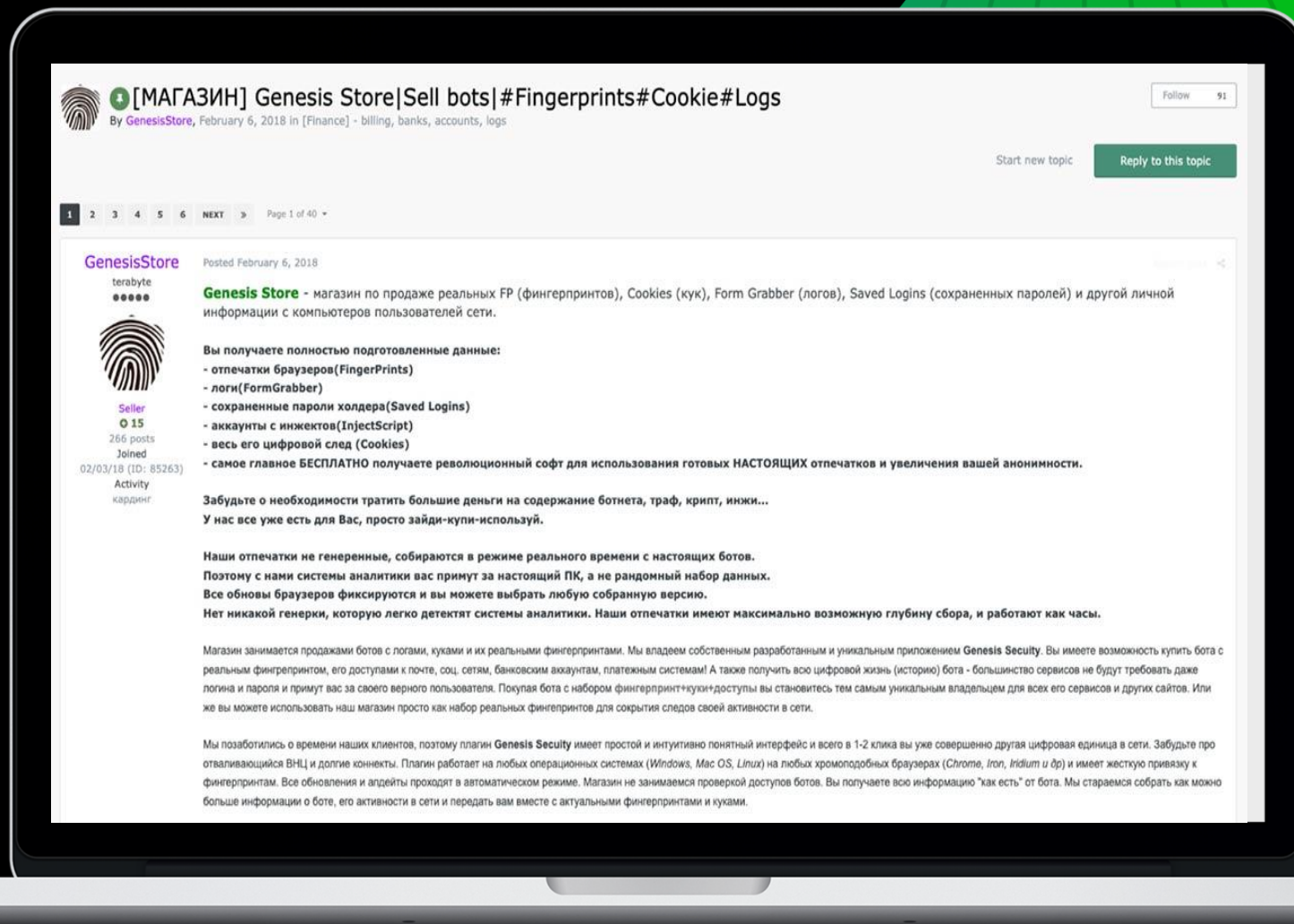


GUARDIA CIVIL



Once upon
a time...

In 2018 on
a Russian
underground
forum.



Trellix

What was in the showroom....

450K different visible profiles

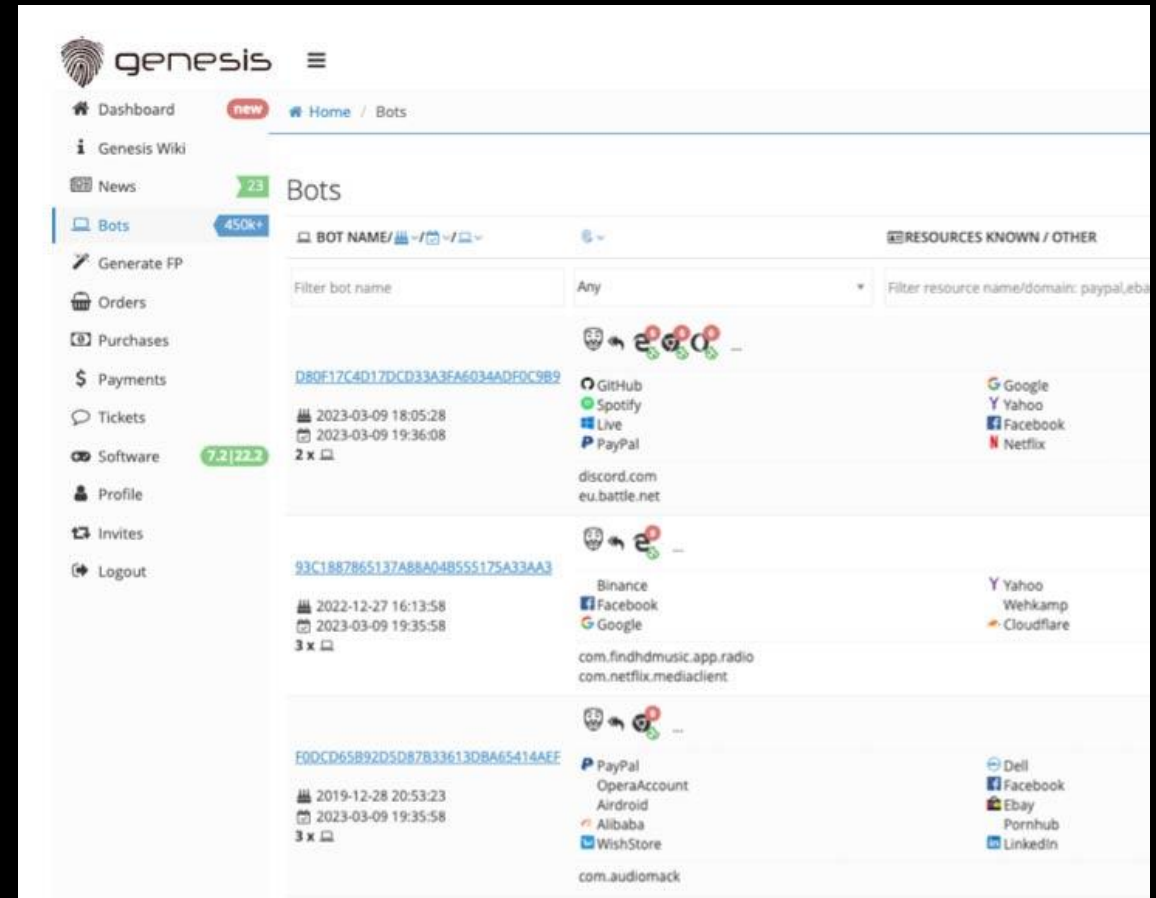
1.5 M Profiles in total

225 Different Countries

6-200 USD Price per Profile

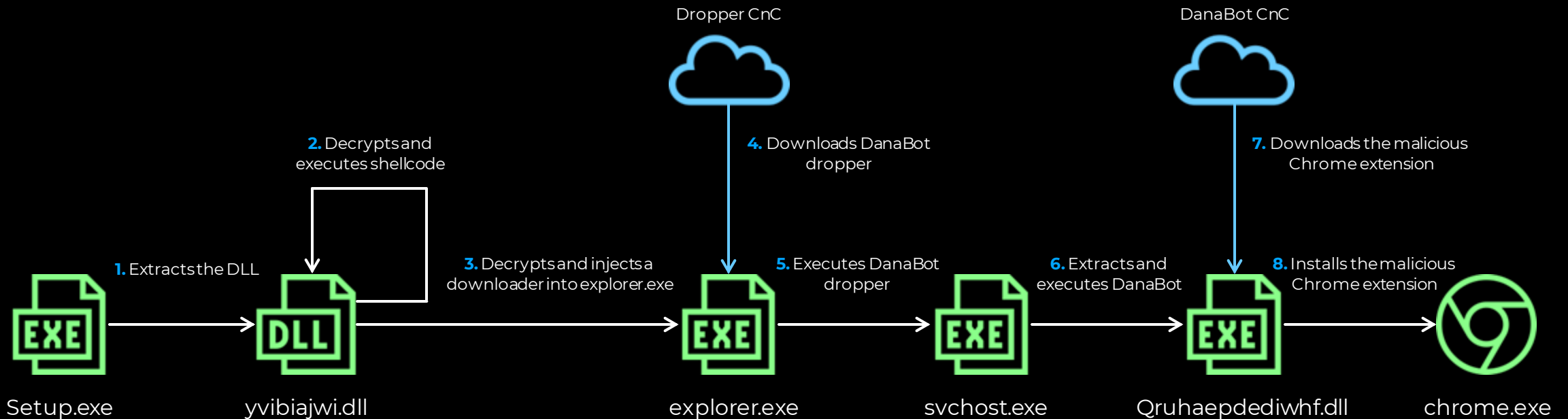
Realtime Updates on the profiles

Access to popular accounts for e.g.:
**Google, Amazon, Facebook, Netflix,
Spotify, PayPal, Alibaba, LinkedIn,
Twitter, Corp logins.... etc.**



How did Genesis keep the showroom full?

Using Commodity malwares and a proprietary browser extension.



Contributions by Trellix:



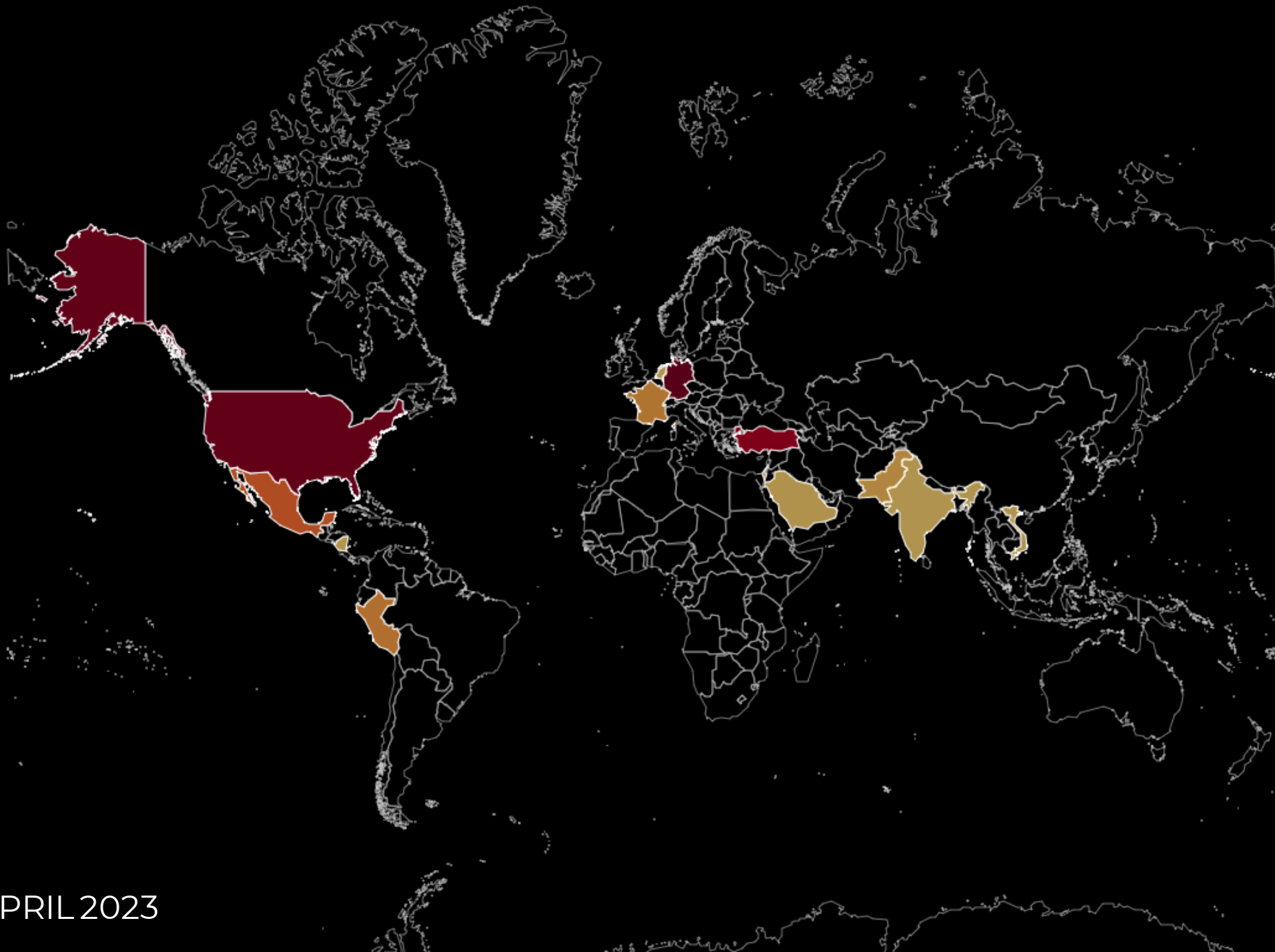
**Malware
Analysis**



**Remediation
Advice**

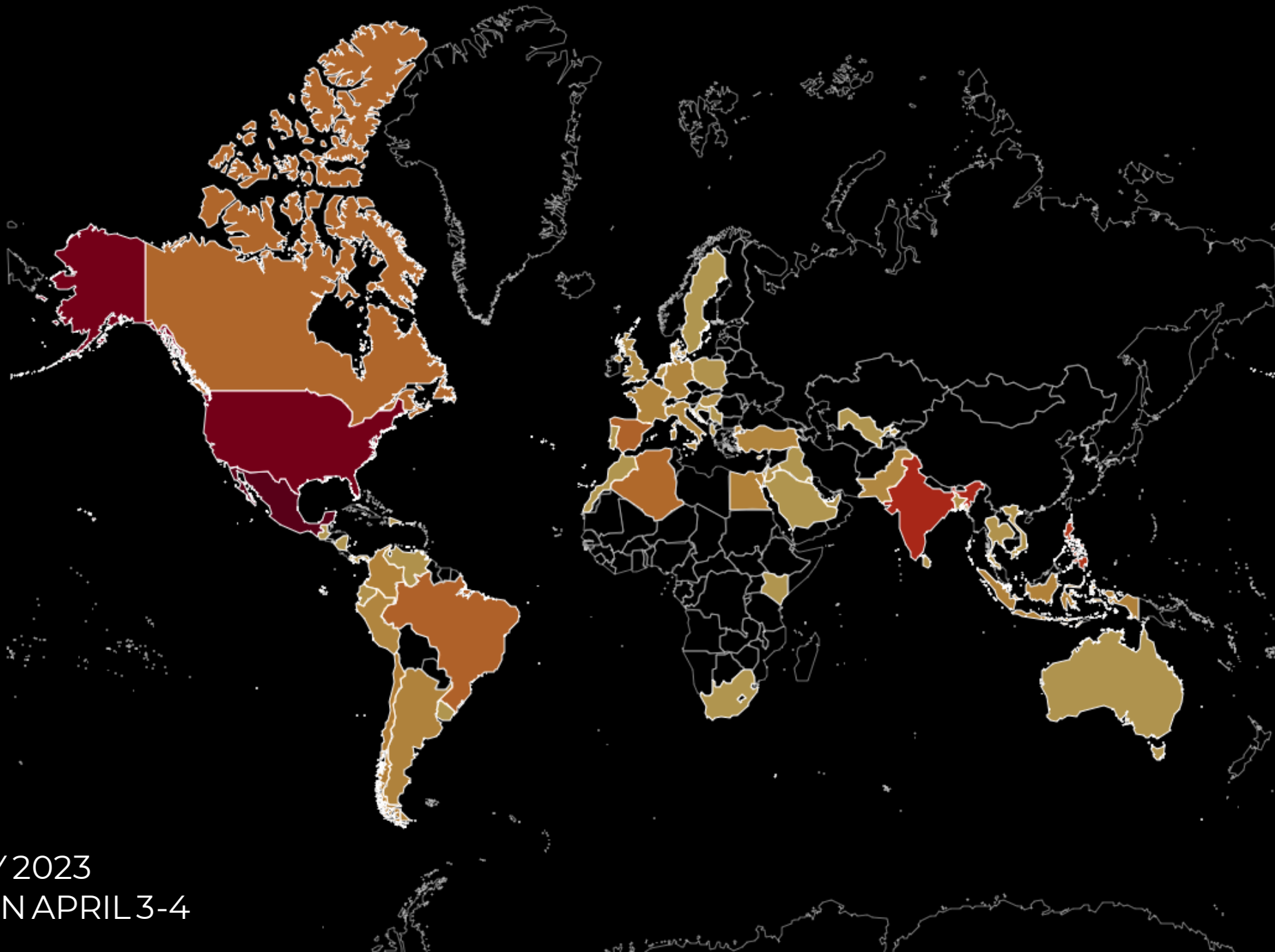


**Sample
Sharing**



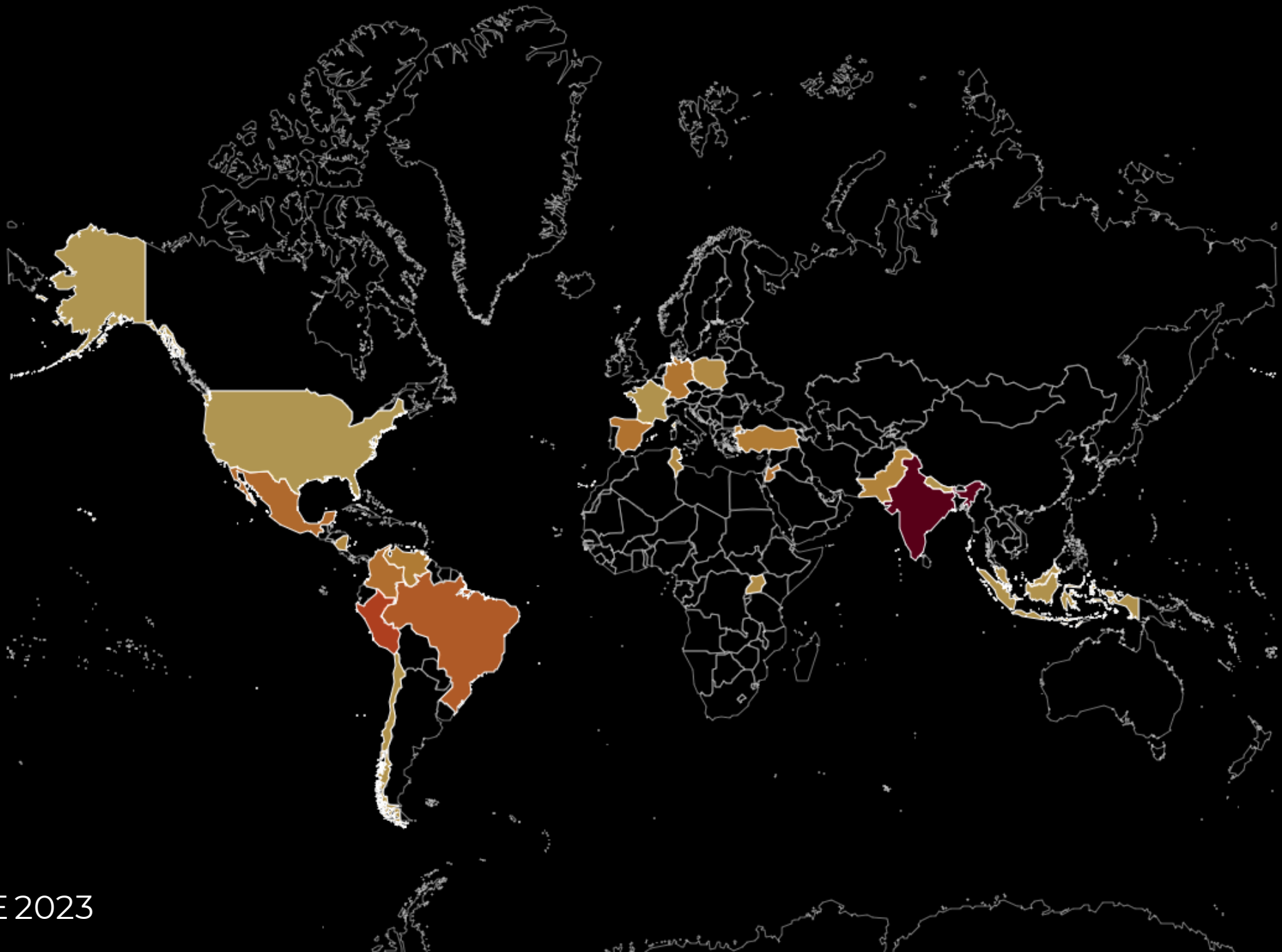
MARCH-APRIL 2023

Trellix



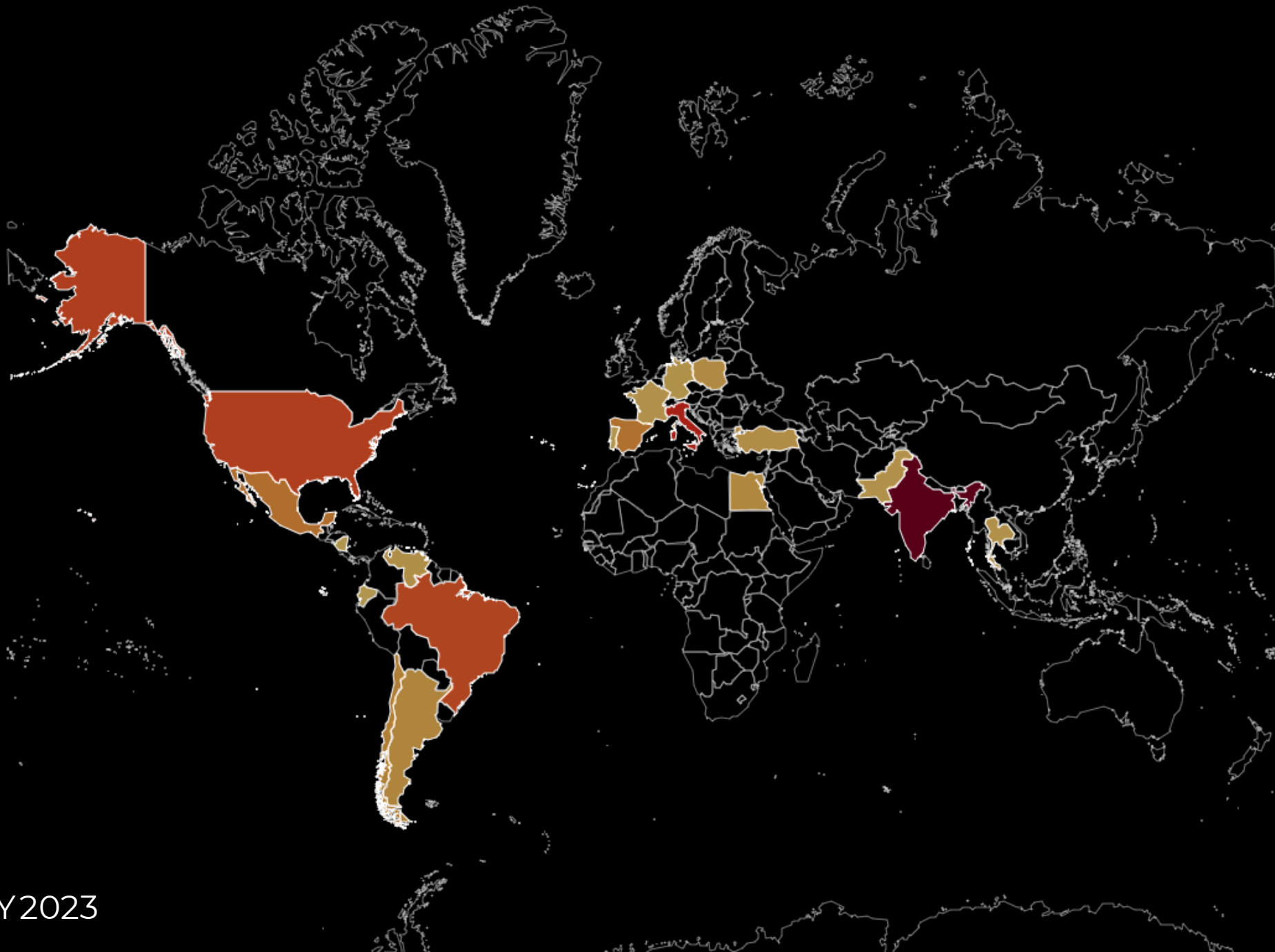
APRIL-MAY 2023
TAKEDOWN APRIL 3-4

Trellix



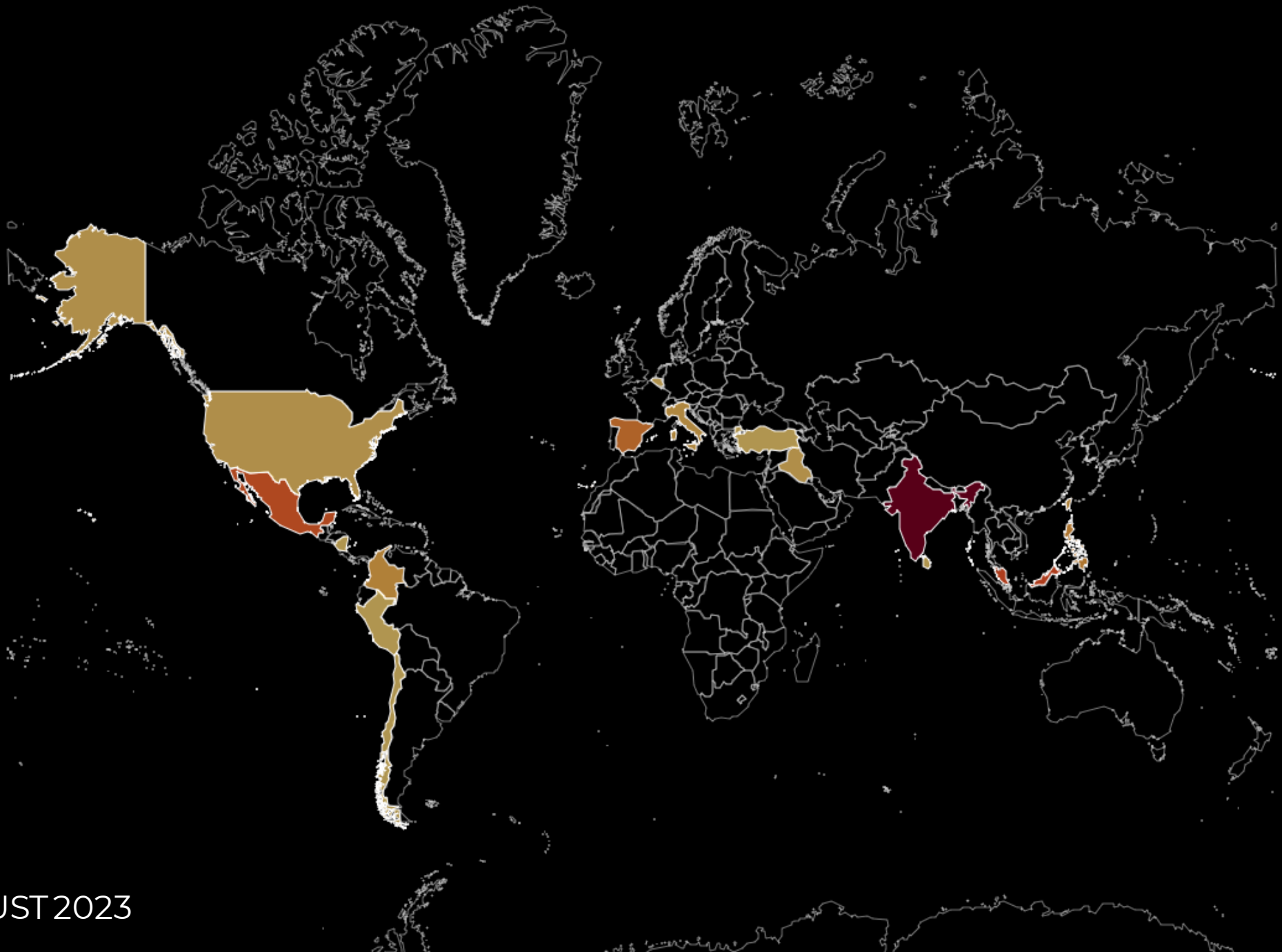
MAY-JUNE 2023

Trellix



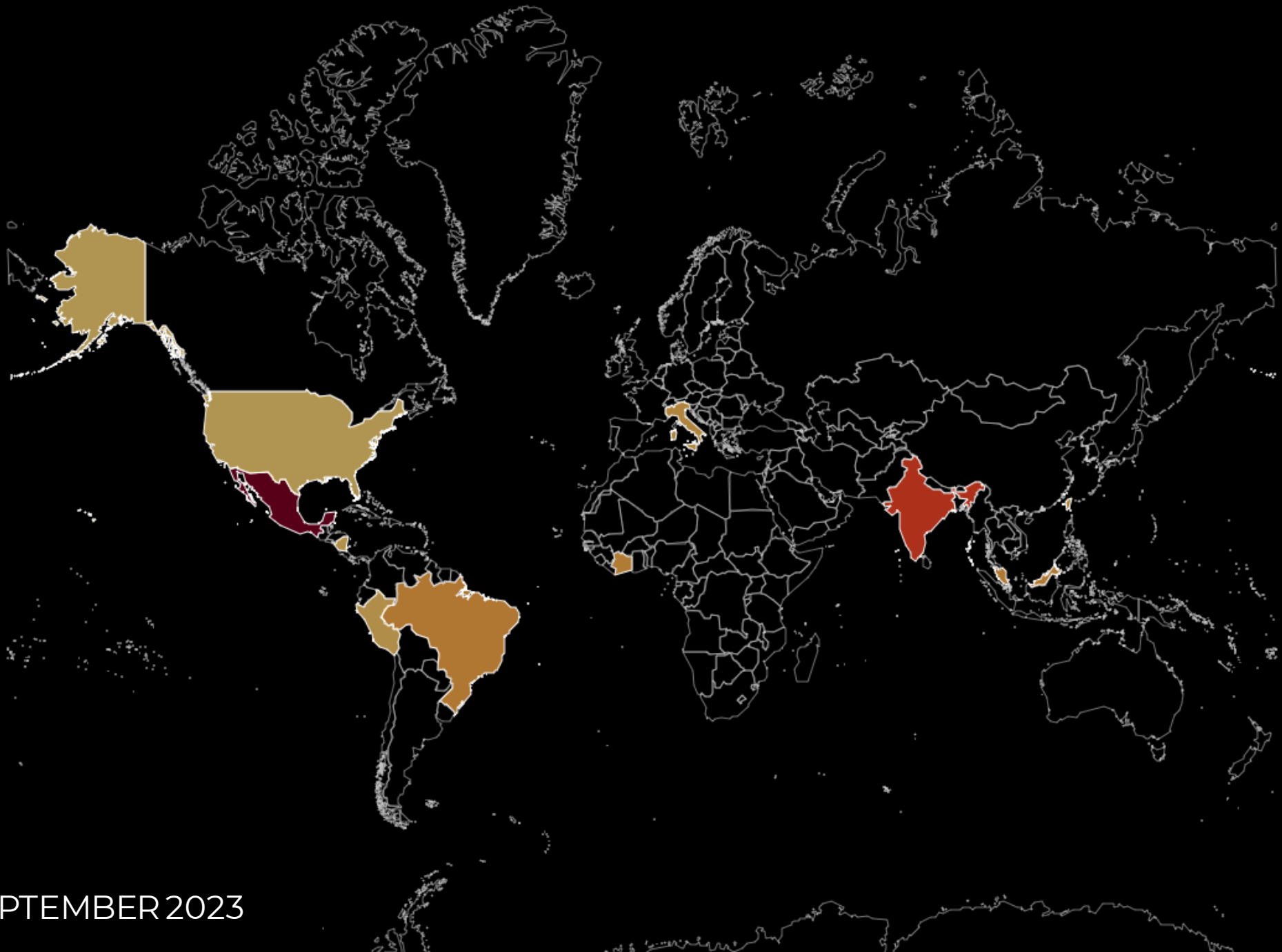
JUNE-JULY 2023

Trellix



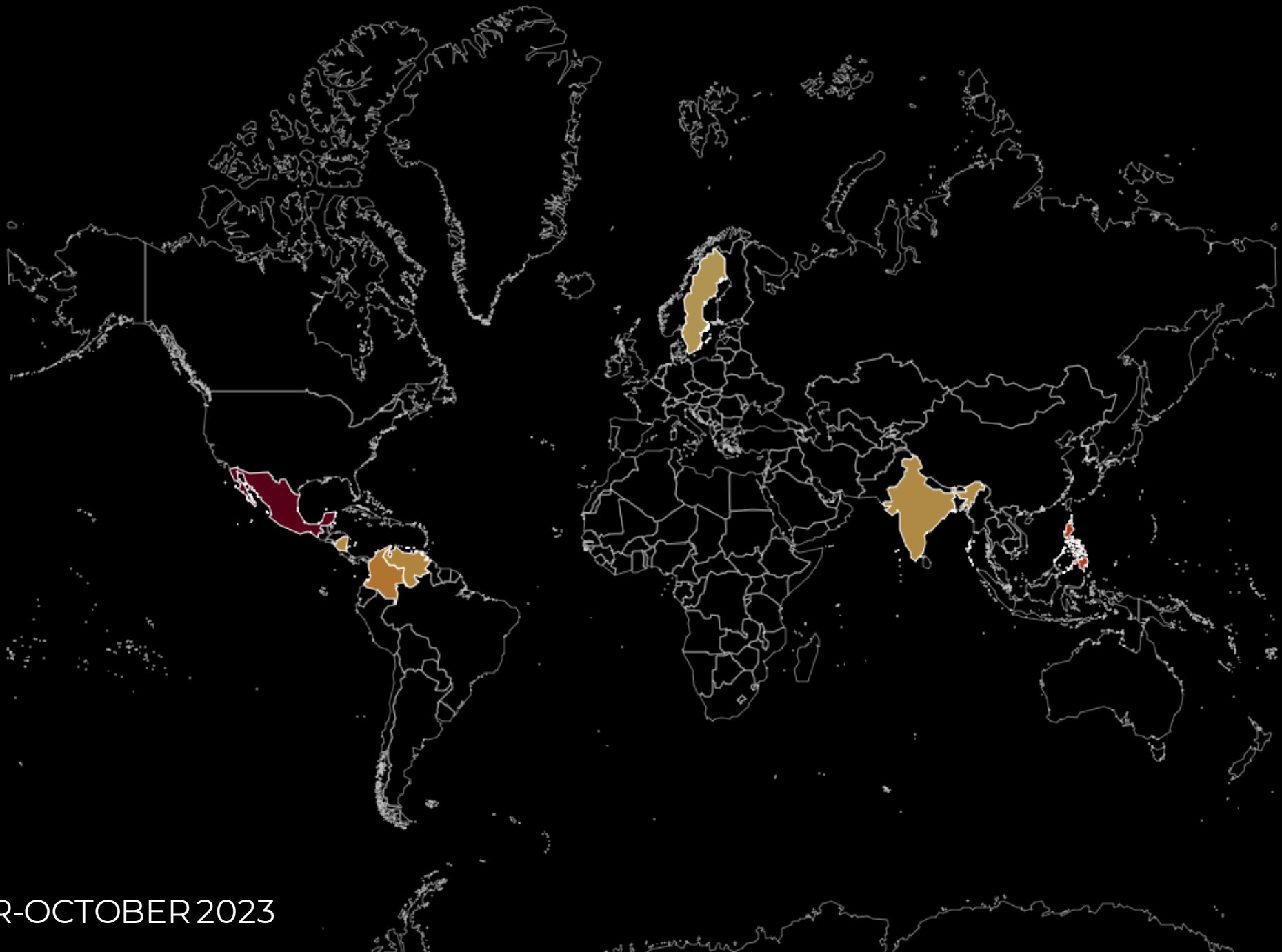
JULY-AUGUST 2023

Trellix



AUGUST-SEPTEMBER 2023

Trellix



SEPTEMBER-OCTOBER 2023

Trellix



Trellix



**What can
you do?**

Trellix

Browser Fingerprint Credential Theft

INDEX SEARCH Start hunting for evil...



PAST 24 HOURS

History Favorites Syntax Help

← BACK

ID# 8870992 | WINDOWS METHODOLOGY [Stored Browser Credential Access]

0 Queues

EXPORT

OPEN

●●● Medium WINDOWS, Browser Credentials, Cookie Access, Credential Access, md-info, Credentials from Password Stores (T1555), Credentials from Web Browsers (T1555.003), OS Credential Dumping (T1003), Steal Web Session Cookie (T1539)

First Seen: 2023-04-24 18:57:50

Last Seen: 2023-04-24 19:45:23

This rule identifies the execution of a process with arguments pointing to known browser files that store passwords and cookies. Adversaries/Malwares may acquire credentials from web browsers by re...

<https://kylemistele.medium.com/stealing-saved-browser-passwords-your-new-favorite-post-exploitation-te...>
<https://attack.mitre.org/techniques/T1555/003/>
<https://attack.mitre.org/techniques/T1003/>
<https://attack.mitre.org/techniques/T1539/>



Most Recent Event | Windows Process

hostname	prvfs01w.ptbcorp.com
msg	an attempt was made to access an...
process	c:\windows\system32\cmd.exe
severity	info
class	ms_windows_event
meta_cbid	888888888

eventid	e:\profiles\xenapp\acampus\win2019v6\upm_profile\ap...
username	xt\ihmaflkibpmigkcoadcmckbfhibefp\def\dawncache
filename	e:\profiles\xenapp\acampus\win2...
deviceid	86925042390c
metaclass	windows

Rule

Name	WINDOWS METHODOLOGY [Stored Browser...]
Rule Pack	Windows
Distinguishers	hostname: prvfs01w.ptbcorp.com
Threshold	1 Event
Interval	Every 1 minute
Query	(metaclass:windows ((class=ms_defender cat...
Pivot Query	detect_ruleids:1.1.3875 hostname=prvfs01...

Managed Defense

Severity	N/A
Status	Informational
Disposition	N/A
Threat Type	N/A
Threat Actors	N/A
Capabilities	N/A
Malware	N/A



Credential Protection in Endpoint



Malware
Prevention
Signatures



Exploit
Prevention
Rules



ATP Credential
Theft Protection
Rules



Logon
Tracker



Windows Event
Streamer

EDR Detects Credential Theft Techniques

Monitoring

5
Total Threats

2
High

0
Medium

3
Low

Threat Prioritization

Threats by Ranking

Filter by keyword

View All

sysmon.exe Sep 12, 20... 10:16:03 AM

reg.exe Oct 2, 2023 12:26:19 PM

reg.exe

Initial trigger Trace detection
First detection Oct 2, 2023 12:26:19 PM
Last detection Oct 2, 2023 12:26:19 PM
Affected devices 1
Age 10 days

Take Action

Process Attributes

First Name
reg.exe

MD5
227F63E1D9008B36BDBCC4B397780BE4

SHA-1
C0DB341DEFA8EF40C03ED769A9001D60
0E0F4DAE

SHA-256
C0E25B1F9B22DE445298C1E96DDFCEAD
265CA030FA6626F61A4A4786CC4A3B7D

Threat Details

Device: client23 Oct 2, 2023 12:26:19 PM 1 affected devices

Threat Behavior

Techniques Observed(1)

MITRE ATT&CK™ Matrix

Suspicious Indicators(1)

Security Account Manager T1003.002 (Credential Access)

Dumped credentials from Windows Registry SAM and SECURITY hives via reg.exe

MITRE

Process Activity

Summary View

cmd.exe

reg.exe

Observed (compare to SANS DFIR)

Image path C:\Windows\System32\reg.exe

Type -

Parent process cmd.exe

Command Line reg save hklm\sam sam.dump

Process ID 456296

Password File Access

Identity Provider integrations in XDR



Azure Active Directory



Duo Auth



Entrust Intellitrust



Okta



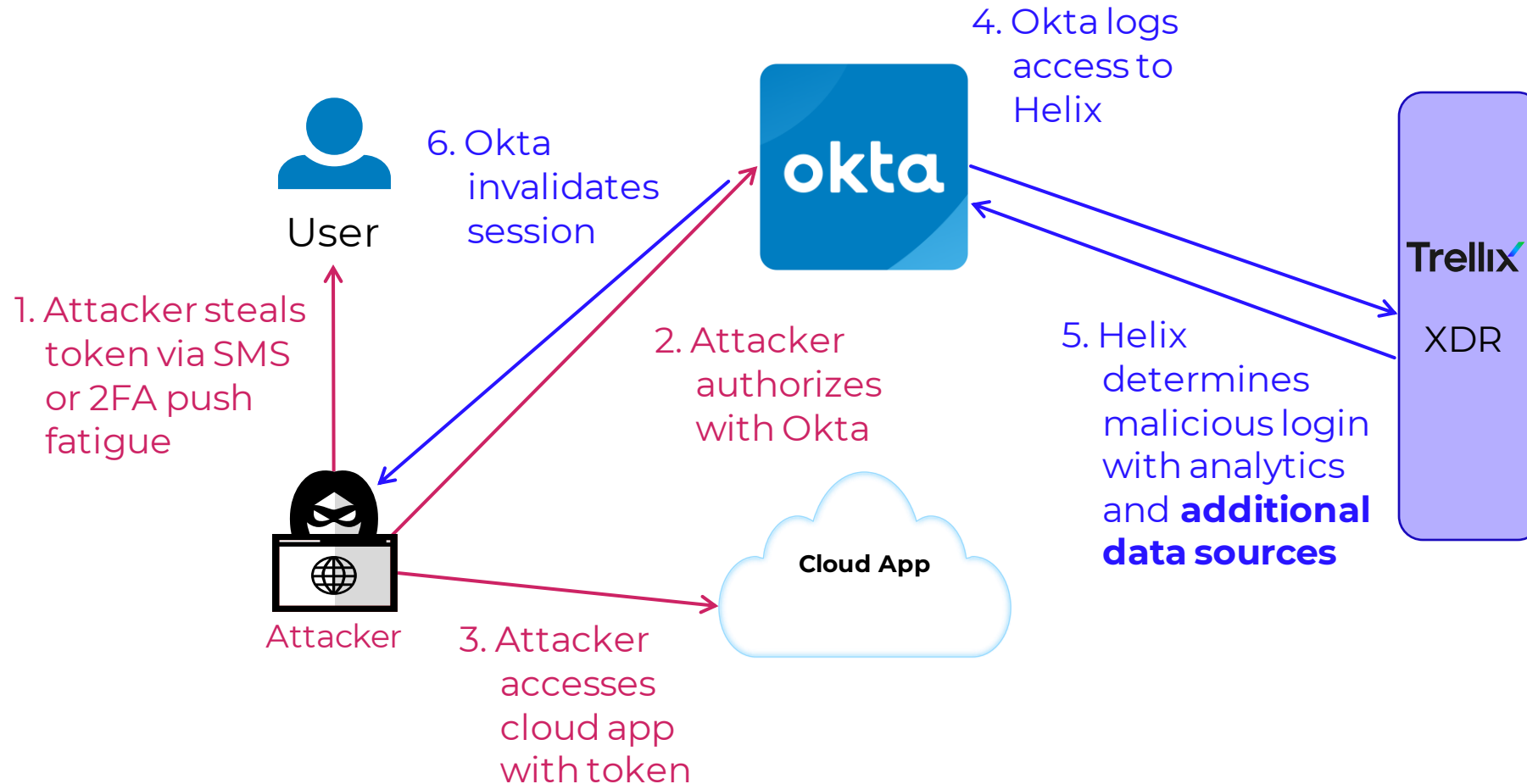
RSA Secure ID



Amazon Verified Access

- ✓ Data Foundation for identity-based scoring in XDR
- ✓ Flag VIP users based on profile for risk scoring
- ✓ Understand authorization levels to apps for a given user
- ✓ Connecting users to roles provides basis for investigations
- ✓ Tracking login patterns informs threat hunting

How can Identity Data + XDR work together?



Chaos to Clarity

Take A Moment is about simply taking a few seconds every day for our mental health...to pause, breath, disconnect and then reconnect, so we can find **Clarity**. A simple action that can make a life changing difference in our fast-paced world.



**WE ALL NEED TO TAKE A MOMENT.
SO, LET'S TAKE A MOMENT TOGETHER.**

Trellix

Thank You!





Trellix and Amazon Web Services (AWS)

Better Together for Cloud Security

Harrison Holstein

Global Solution Architect

The most secure, extensive, and reliable Global Cloud Infrastructure

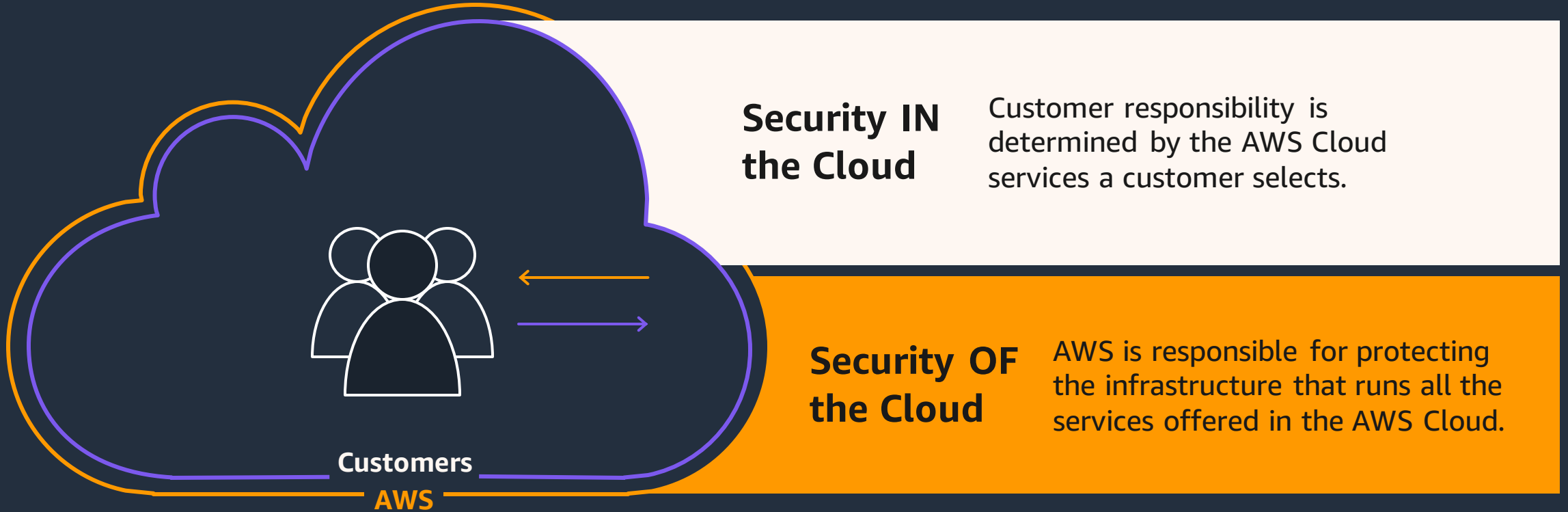
Infrastructure allows you to run workloads

You have the same access and capabilities no matter where you are

200+ fully featured services from data centers globally



Shared responsibility model



Infrastructure & services to elevate your security



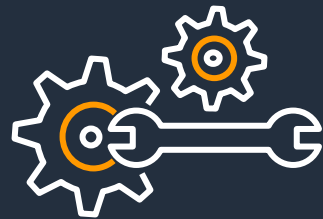
Inherit global security and compliance controls



Scale with superior visibility and control



Highest standards for privacy and data security



Automate & reduce risk with deeply integrated services



Largest ecosystem of security partners and solutions

Highest standards for privacy and data security



Meet data residency requirements

Choose an AWS Region, and AWS will not replicate it elsewhere unless you choose to do so



Encryption at scale

with keys managed by AWS Key Management Service or manage your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs



Comply with local data privacy laws

by controlling who can access content, its lifecycle, and its disposal



Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Further and faster, together

COMMITMENT

On September 19, 2019, Amazon and Global Optimism announced The Climate Pledge, a commitment to meet the Paris Agreement 10 years early

THE Paris...
CLIMATE 10 years
PLEDGE Early

Net-zero carbon by 2040

Path to 100% renewable energy by 2025

\$2 billion Climate Pledge Fund

THE Paris... CLIMATE 10 years PLEDGE Early

PRINCIPLES

Regular
reporting

Carbon elimination

Credible offsets

PROGRESS

200+
signatories

26
industries

21
countries

Alaska
AIRLINES

BNB
BNBuilders

Coca-Cola

CP
COLGATE-PALMOLIVE

EST. 1873
Heineken®

IBM

IRON
MOUNTAIN®

LifeStraw

Lime

posti

RUSSELL
GROUP

Telefónica

Unilever

VISA



It's more
sustainable
in the cloud

3.6x

More energy efficient

88%

lower carbon footprint

Trellix

&

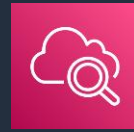


Trellix and AWS

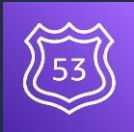
Trellix and Amazon Web Services (AWS) have come together to expand security capabilities on the cloud and uncover cloud-specific threats.



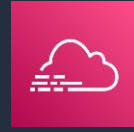
AWS Network Firewall



Amazon CloudWatch



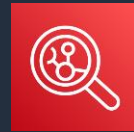
Amazon Route 53 Resolver
DNS Firewall



AWS CloudTrail



Amazon Virtual Private Cloud
(Amazon VPC) Flow Logs



Amazon Inspector



AWS Verified Access



Amazon Guard Duty



Amazon Simple Storage Service
(Amazon S3)



AWS Security Hub

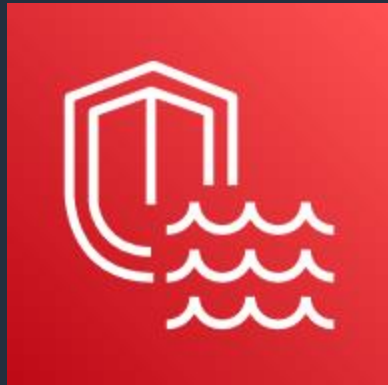


Amazon Security Lake



Amazon Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE



Breakout 8 – Thursday 26 October
11:45-12:40

Automatically centralize data from AWS environments, SaaS providers, on premises, and cloud sources across AWS Regions

Optimize and manage security data for more efficient storage and query performance

Normalize data to an open standard to streamline security data management across multicloud and hybrid environments

Analyze security data using your preferred analytics tools while retaining complete control and ownership of that data

NOW GENERALLY AVAILABLE

Amazon Bedrock

The easiest way to build and scale generative AI applications with foundation models (FMs)



Accelerate development of generative AI applications using FMs through an API, without managing infrastructure



Choose FMs from Amazon, AI21 Labs, Anthropic, Cohere, Meta, and Stability AI to find the right FM for your use case



Privately customize FMs using your organization's data

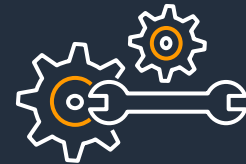
Keeping your data private and secure



None of the customer's data is used to train the underlying model

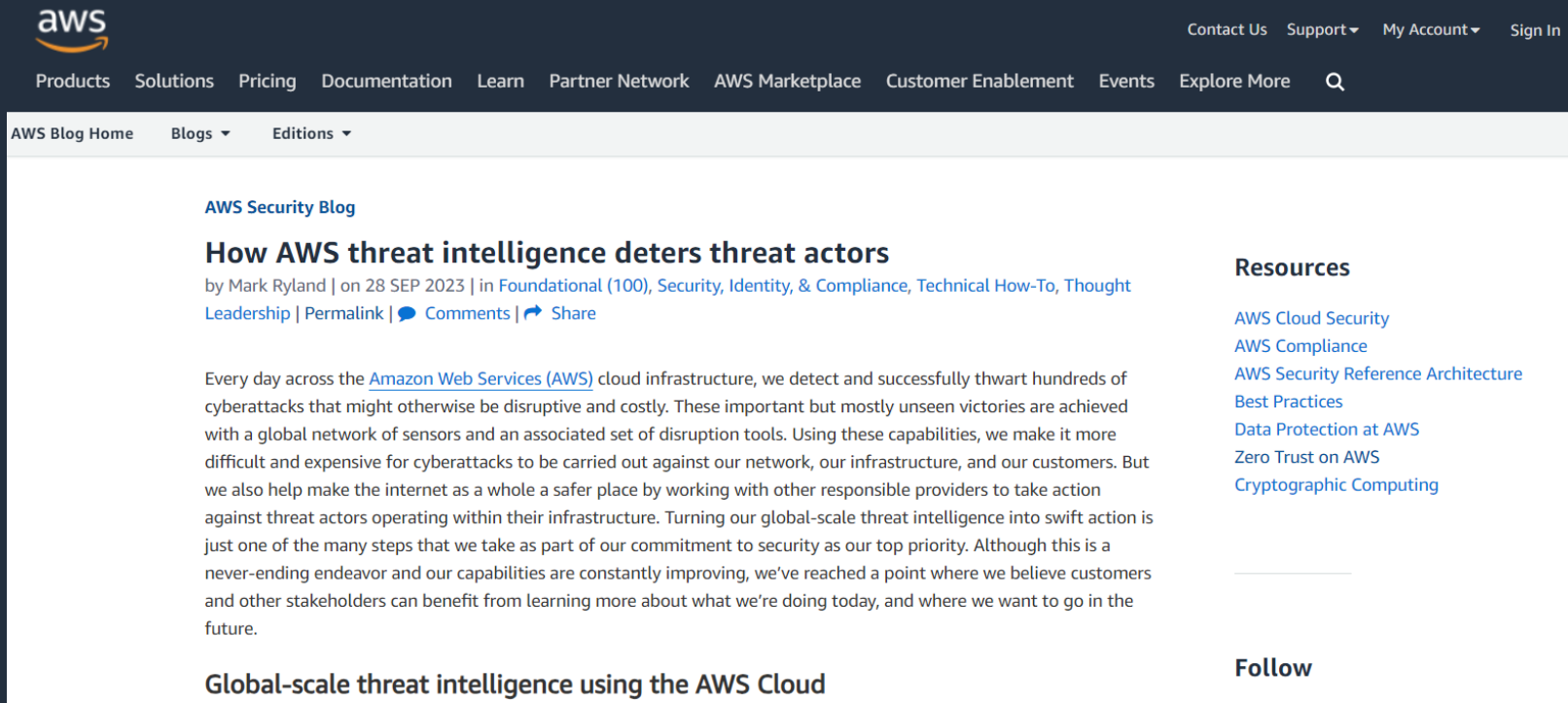


All data is encrypted at rest and PrivateLink support allows access to Bedrock APIs via customer's VPC endpoints



Customized foundation models and the customer-specific data that trains them remain private

AWS threat intelligence



The screenshot shows the AWS Security Blog page for the article "How AWS threat intelligence deters threat actors". The page includes the AWS logo, navigation links (Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, Customer Enablement, Events, Explore More), and user options (Contact Us, Support, My Account, Sign In). The article is by Mark Ryland, dated 28 SEP 2023, and is categorized under Foundational (100), Security, Identity, & Compliance, Technical How-To, Thought Leadership. The main text discusses how AWS cloud infrastructure detects and thwarts cyberattacks. A QR code is visible on the right side of the page.

AWS Security Blog

How AWS threat intelligence deters threat actors

by Mark Ryland | on 28 SEP 2023 | in [Foundational \(100\)](#), [Security, Identity, & Compliance](#), [Technical How-To](#), [Thought Leadership](#) | [Permalink](#) | [Comments](#) | [Share](#)

Every day across the [Amazon Web Services \(AWS\)](#) cloud infrastructure, we detect and successfully thwart hundreds of cyberattacks that might otherwise be disruptive and costly. These important but mostly unseen victories are achieved with a global network of sensors and an associated set of disruption tools. Using these capabilities, we make it more difficult and expensive for cyberattacks to be carried out against our network, our infrastructure, and our customers. But we also help make the internet as a whole a safer place by working with other responsible providers to take action against threat actors operating within their infrastructure. Turning our global-scale threat intelligence into swift action is just one of the many steps that we take as part of our commitment to security as our top priority. Although this is a never-ending endeavor and our capabilities are constantly improving, we've reached a point where we believe customers and other stakeholders can benefit from learning more about what we're doing today, and where we want to go in the future.

Global-scale threat intelligence using the AWS Cloud

Resources

- [AWS Cloud Security](#)
- [AWS Compliance](#)
- [AWS Security Reference Architecture Best Practices](#)
- [Data Protection at AWS](#)
- [Zero Trust on AWS](#)
- [Cryptographic Computing](#)

Follow





Thank you!

AWS@trellix.com

Panel Discussion

Cybersecurity Landscape | EMEA Perspective



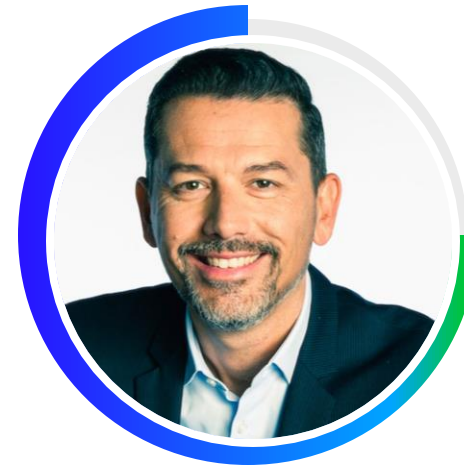
Fabien Rech

Trellix
SVP and GM
EMEA



Michael Faulkner

NATO
Deputy Head
Infrastructure



Chris Steiner

Zimperium
Vice President
EMEA



Vibin Shaju

Trellix
VP, Solutions Engineering
EMEA